International Journal of Digital Crime and Forensics
Volume 13 • Issue 2 • March-April 2021

Fragile Watermarking Framework for Tamper Detection of Color Biometric Images

Rohit Thanki, Prognica Labs, Dubai, UAE
https://orcid.org/0000-0002-0645-6266
Surekha Borra, K. S. Institute of Technology, India
Ashish Kothari, Atmiya University, India

ABSTRACT

Application of fragile watermarking on biometric images stored at a server or cloud ensures proper authentication and tamper detection when access to the servers was shared. In this paper, a hybrid domain fragile watermarking technique for authenticity of color biometric images, using hybridization of various transforms such as discrete cosine transform (DCT), fast discrete curvelet transform (FDCuT), and singular value decomposition (SVD) is proposed. The hybrid transform coefficients are modified according to the scrambled color watermark to obtain watermarked color biometric image. The security of this technique is strengthened with the usage of Arnold scrambling, and by using multiple secret keys. The proposed technique is analyzed on FEI Brazilian face database. The experimental results show that this technique performs better than the existing fragile watermarking techniques.

KEYWORDS

Authentication, Biometric, Color Image, Face, Iris, Server, Tamper Detection, Watermarking

1. INTRODUCTION

Today, the biometric based systems are used everywhere for individual recognition. The biometric systems overcome the limitation of traditional identification systems which are based on password, token, and identity card (Jain and Kumar, 2002). The biometric modalities can be physical or behavioral which includes face, fingerprint, iris, speech and signature etc. The drawback of this system is that it is possible that the biometric image or template can be modified by imposter at system database or while sharing (Ratha et al., 2001; Jain and Uludag, 2003a, 2003b; Jain et al., 2004; Jain and Uludag, 2002; Jain et al., 2002; Rege, 2012). Many information hiding approaches such as cryptography, steganography, and watermarking are used for protection of biometric images against such spoof attacks (Ratha et al., 2001).

DOI: 10.4018/IJDCF.2021030103

This article, published as an Open Access article on February 15, 2021 in the gold Open Access journal, The International Journal of Digital Crime and Forensics (IJDCF) (converted to gold Open Access January 1, 2021), is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

In biometric as a service (BAAS), biometric databases are stored on servers, and are capable of authentication and identification of biometrics on request demand. This has similar setup as any traditional web service; however, at the client level, biometric scanners are used for acquisition of biometric data. There are two types of services: enrolment and identification. In case of enrolment of a user, his or her biometrics is scanned and is associated with the unique identity number before storing in server. For identification, a user is scanned again for his or her biometrics. The system sends identification requests to server, which would return a match or no-match, based on which, a user is allowed to access or deny the application. The security of biometrics is vulnerable at system database due to spoof attacks (Jain and Kumar, 2002; Ratha et al., 2001; Jain and Uludag, 2003a; Jain et al., 2004).

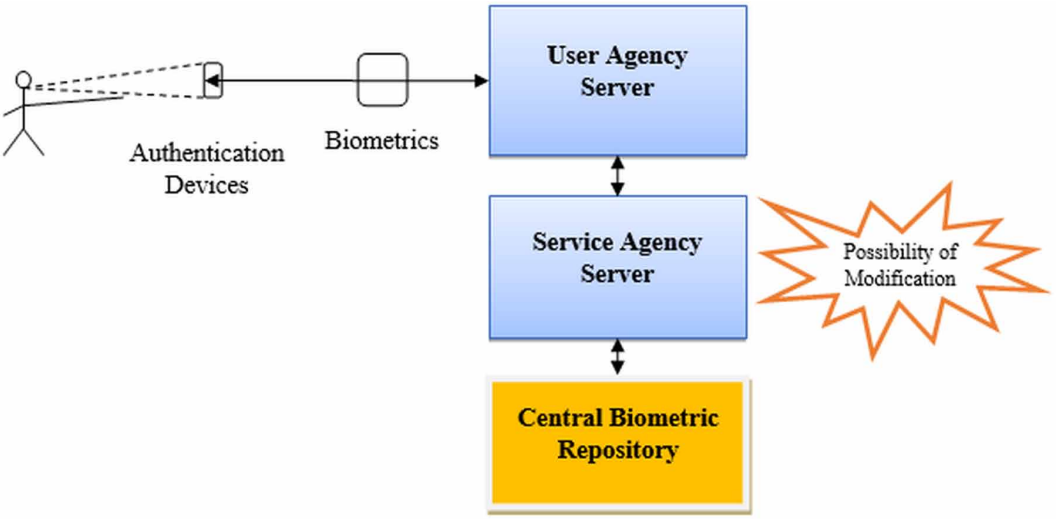
With the rapid growth in the technology, more than 60 countries worldwide are acquiring, storing and using the biometric data of their citizens, for various purposes. "Aadhaar", the name used to represent "The Unique Identification Authority of India (UIDAI)", is the world's biggest biometric database (over 1.1 billion users face, fingerprint and iris images), and is now facing a serious problem of unauthorized access to its database. Aadhaar started out as a voluntary programme to help tackle benefit fraud, but recently it has been made mandatory for access to welfare schemes, pensions and rural employment schemes, tax filing and is linked to bank accounts and mobile phone numbers. The Aadhar identity number has cut wastage, removed fakes, curbed corruption and made substantial savings for the government.

The government of India hired service providers for grievance redress, whose agents are allowed to enter any Aadhaar number into the UIDAI website and get access and rectifies user information including name, address, photo, biometrics, phone number and email address. It was reported recently that the citizen's personal data was sold online by the agents. Poor security at four government portals revealed personal and bank account details of around 13 Crore people. The government itself has admitted that it has blacklisted or suspended some 34,000 service providers for helping create "fake" identification numbers or not following proper processes. The theft of such personal details has become very common due to lack of privacy laws, architectures and lack of information security practices. It is also reported in news, that the biometrics databases around the world, are stolen and are or misused (BBC News Article, 2016; BBC News Article, 2015). This is due to the fact that the biometrics, when linked to bank accounts and financial services leads to rise in committing the frauds, as it is possible for the biometrics such as fingerprints to be stolen and collected and copied from the public places (The Hindu Business Line Article, 2017; Unique Identification Authority of India, 2016). [https://www.uidai.gov.in/authentication/authentication-overview/operation-model.html]. In such scenario, it is the need of the hour, securing the biometrics and personal data, stored in and shared by the servers.

Encryption which comes first in Digital Rights Management ensures access control and authentication of users or content. The Aadhar programme for example secures the collected demographic and biometric information of citizens by means of advanced encryption using a 2048-key. Cryptographic techniques make the content unintelligible using encryption keys and algorithms, before its storage/publication/ distribution. But, the person or device having the knowledge of the decryption key is allowed to access and decrypt completely the encrypted data upon checking his authorization and user rights, and can tamper or make copies, as in Fig. 1. The encryption techniques cannot copy control once the data is decrypted. The watermarking techniques on the other hand can protect and copy control data even after decryption. The fragile watermarking embeds marks in imperceptible portions of image such that the marks get destroyed in case of modifications/tampering of the image indicating the same. The objective of fragile marking is to ensure if that the host image is tampered, and that the data integrity and authentication is maintained. Fragile marks are useful as evidence that the image is modified.

In this paper, a fragile watermarking scheme is proposed for authenticity verification and tamper detection of biometric images. A key, which is maintained confidentially by authorized personnel/

Figure 1. Possible tampering of biometric images



server owner, is used for watermark extraction non-blindly when required. Successful watermark extraction indicates the authentication of authorized person, and data integrity. The rest of the paper is organized as follows: in section 2, some related work is given, section 3 reviews some preliminaries. Section 4 discusses the proposed color biometric watermarking technique. Experimental results along with analysis are presented in section 5 and finally, conclusions are stated in section 6.

1.1 Related Work

Many fragile watermarking techniques have been proposed in the literature for authenticating and tamper detection of biometric images during their transmission or while storing them at server or system database.

D. Wang (Wang et al., 2008) proposed fragile watermarking technique based on SVD for integrity verification of biometric image. In this technique, singular values of watermark bits are inserted into Least Significant Bits (LSB) of biometric mage. This technique was implemented on greyscale iris images. C. Li (Li et al., 2010; Li et al., 2012) proposed two fragile watermarking techniques based on LSB substitution for tamper detection and recovery in biometric images. In the first technique, a multi-level approach is used for integrity verification. The PCA features of biometric image are used for recovery of tampered region in an image. The authentication bits and watermark bits are inserted into gray scale face biometric images based on salient region detection and adaptive watermarking. In the second technique, cover biometric image was divided into two regions: salient and background. The salient regions have rich information; less affected by the watermark, and thus allows large watermarks to be embedded into it.

Yang (Yang and Shen, 2010) proposed fragile watermarking technique based on vector quantization (VQ) for tamper detection and recovery in biometric images. The index table of cover biometric image is generated using vector quantization method and these table values are used as watermark. The watermark values are embedding into the cover biometric image for recovery of the tamper region in the image. This technique is the modified version of Wong's watermarking technique (Wong and Memon, 2001). C. Li (Li et al., 2013) proposed fragile watermarking technique based on multi-block dependency for tamper detection of biometric images. In this technique, the biometric image is first divided into non-overlapping blocks of size 8×8. A 64-bit watermark is generated for each block of image and is divided into eight equal parts. Each part of the watermark is inserted into

another block of image using secret key. This technique was implemented on gray scale fingerprint images.

M. Joshi et al. (2013) proposed a multilevel semi-fragile watermarking technique for fingerprint images based on Singular Value Decomposition (SVD). This technique embeds two watermarks for providing protection of biometric image at system database, and at matcher of biometric system. In this technique, watermark 1, derived using block based singular values of cover biometric image is used for authentication. The watermark 2 derived using 2nd and 3rd order moments of cover biometric image is used for the security of features at matcher and to provide resistance against affine transformation and lossy compression. The authors extended their work and proposed a reversible technique in 2016 (Joshi et al., 2016). V. Joshi et al. (2013) proposed a fragile watermarking technique based on Multistage Vector Quantization (VQ) and DCT for tamper detection of biometric images. C. Whitelam (Whitelam et al., 2013) proposed watermarking technique for authentication of biometric image. In this technique, face image is inserted into fingerprint image to generate watermarked fingerprint image, which is further inserted into color standard image using steganography. The Riverst-Shamir-Adleman (RSA) encryption is used for encryption of stego color image for secure transmission.

R. Preda (Preda, 2013) proposed fragile watermarking technique based on wavelet transform for tamper detection of biometric images. In this technique, the watermark bits are inserted into randomly chosen wavelet coefficients of gray scale face biometric images. V. Joshi (Joshi, 2014) proposed watermarking technique based on LSB substitution and encryption for authentication of biometric image. Bit slicing is applied on cover biometric image, and each bit plane is converted into vectors, before encryption. The encrypted vectors are converted into encrypted bit plane. The watermark bits are inserted into LSB of encrypted image using LSB substitution method. This technique was implemented on grayscale fingerprint images.

C. Li (Li et al., 2016) proposed fragile watermarking technique using singular value decomposition (SVD), principal component analysis (PCA) and wavelet transform for tamper detection and recovery of biometric image. In this technique, the authentication watermark bits are generated using SVD for each block of cover biometric image and the information watermark bits are generated using PCA. Both these watermarks are inserted into wavelet coefficients of block using wavelet quantization approach. After detecting tamper regions using authentication bits, the tampered region is recovered using information watermark bits. A. Czajka (Czajka et al., 2016) proposed fragile watermarking technique based on discrete cosine transform (DCT) for authentication of biometric image. The image is first divided into non-overlapping blocks, followed by application of DCT and is then divided into two types of bits: signable bits and embeddable bits, where the signable bits are used to generate hash watermark bits. The watermark bits are inserted into embeddable bits of DCT coefficients. This technique is implemented for gray scale iris image.

A fragile watermarking technique based on SVD is proposed for color biometric image authentication by E. Tarif (Tarif et al., 2017). In this technique, sparse data generated using sparse decomposition method is inserted as watermark into singular value of luminance component of color face biometric image. A. Tiwari (Tiwari et al., 2017) proposed fragile watermarking technique based on vector quantization, for authentication of biometric images. In this technique, two stage watermark embedding process is performed for integrity verification and authentication of image. In the first stage, robust watermark is inserted into vector quantized indices of cover image using zero level watermarking method. In the second stage, semi-fragile watermark is inserted using modified index key-based method.

From the literature, it is observed that there are very less number of fragile watermarking techniques defined for authentication of color biometric images. Taking this as motivation, in the paper, a color biometric watermarking technique is proposed based on hybridization of discrete cosine transforms (DCT), fast discrete curvelet transform (FDCuT), and singular value decomposition (SVD). The proposed watermarking technique inserts color watermark into chosen hybrid coefficients of cover biometric image. The combination of DCT + FDCuT + SVD provides required fragility. The

authentication of watermarked color biometric image is performed based on measuring the similarity between extracted watermark and original watermark information. The main features of the proposed technique include: (1) Utilization of hybrid coefficients which carry the properties of DCT, FDCuT, and SVD (2) Encryption of watermark using Arnold Scrambling (3) Good trade-off between perceptual transparency and payload capacity. (4) Tamper detection in case of attacks. (4) Outperforms existing fragile biometric watermarking techniques in terms of perceptual transparency and security.

2. PRELIMINARIES

In this section, the operations used in the design of proposed technique are reviewed. These include Discrete Cosine Transform (DCT), Fast Discrete Curvelet Transform (FDCuT), Singular Value Decomposition (SVD), and Arnold scrambling.

2.1 Discrete Cosine Transform

For any digital image, the DCT and inverse DCT are calculated using Equations 1 and 2, respectively (Leng et al., 2010a, 2010b; Roy and Pal, 2017; Jain, 1999). The DCT can be applied on the entire image or on the blocks obtained from the image.

$$F(u,v) = a(u)\cdot a(v)\sum_{x=1}^{M-1}\sum_{y=1}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2M}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (1)$$

where, $a(u) = \sqrt{1/M}$ for u = 0; $a(u) = \sqrt{2/M}$ for u = 1, 2, 3… M-1; $a(v) = \sqrt{1/N}$ for v = 0; $a(v) = \sqrt{2/N}$ for v = 1, 2, 3 … N-1:

$$f(x,y) = \sum_{x=1}^{M-1}\sum_{y=1}^{N-1} a(u)\cdot a(v)\cdot F(u,v)\cos\left[\frac{(2x+1)u\pi}{2M}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (2)$$

In the proposed technique, DCT is independently applied on all the three channels of the cover color face image to obtain frequency sub-bands: low, middle and high, into which the color fragile watermarks, are inserted.

2.2 Fast Discrete Curvelet Transform (FDCuT)

Curvelet Transform (CuT) (Candes et al., 2006; Candes and Donoho, 2004) is applied on the image to obtain various curvelet subbands with varying frequency coefficients. The CuT plays an important role in image processing applications, representing image as curves or edges. The discrete time curvelet transform (DTCT) is redesigned with a new mathematical architecture, which is simple and easy to be implemented. It is known as Fast Discrete Curvelet Transform (FDCuT) (Candes et al., 2006; Candes and Donoho, 2004). There are two types of FDCuT: frequency wrapping based and unequispaced Fast Fourier transform (USFFT) based.

Discrete Cosine Transform (DCT) represents image in terms of its spatial frequency but requires large number of coefficients to represent the image. The sparsity property of FDCuT describes the image accurately using few coefficients with less computational complexity. In the proposed technique, FDCuT is applied on DCT coefficients of all the three channels (RGB) of the cover color face image independently to result hybrid frequency curvelet coefficients: LF, MF and HF. In order to achieve higher transparency with the proposed technique, high frequency (HF) curvelet coefficients are considered for inserting the color watermark image.

2.3 Singular Value Decomposition

The Singular Value Decomposition (SVD) is a linear algebra tool which decomposes the image into three different matrices: a singular value matrix and two orthogonal matrices namely, U matrix and V matrix. The singular value matrices have non-negative values and are diagonally placed in the matrix. The singular values are very stable in nature and are less affected by the general image manipulations. In the proposed technique, SVD is used to maintain the stability of hybrid coefficients and ensure that the watermark embedding process is perfectly invertible.

2.4 Arnold Scrambling

In the proposed watermarking technique, Arnold scrambling (Li et al., 2013; Roy and Pal, 2017) is used to encrypt the color watermark image before it is embedded into the cover color biometric image. So that attacker or impostor cannot directly obtain watermark information from the watermarked color biometric image. The resultant chaotic image is secure and cannot be extracted without the knowledge of the secure key. The 2D forward Arnold scrambling is defined by the equation:

$$\begin{vmatrix} x' \\ y' \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} \begin{vmatrix} x \\ y \end{vmatrix} \bmod N \tag{3}$$

where, $x, y, x', y' = \{0, 1, 2\ldots N-1\}$; i, j are the pixel coordinates of the original space; x', y' are the pixel coordinates after iterative computation scrambling; and N is the size of the watermark image.

The original watermark image is obtained back by inverse Arnold scrambling as follows:

$$\begin{vmatrix} x \\ y \end{vmatrix} = \left(\begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} \begin{vmatrix} x' \\ y' \end{vmatrix} + \begin{vmatrix} N \\ N \end{vmatrix} \right) \bmod N \tag{4}$$

3. PROPOSED WATERMARKING TECHNIQUE

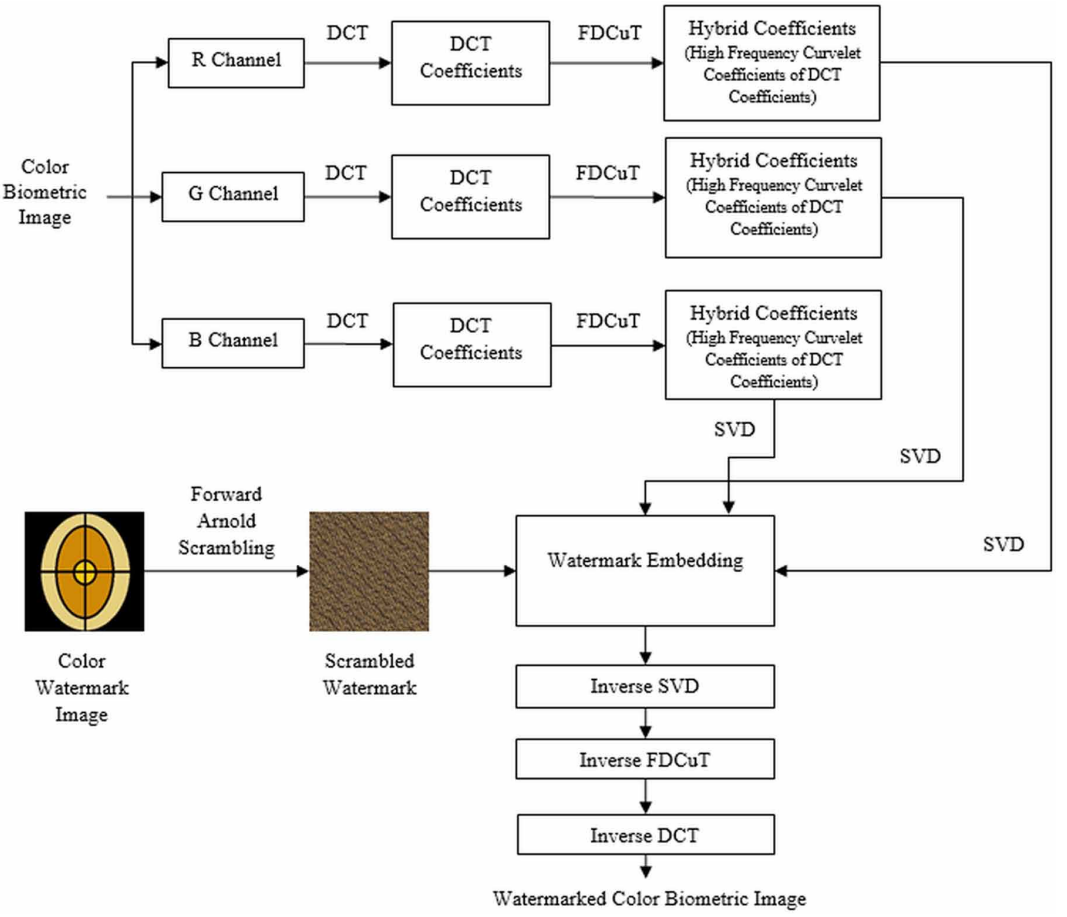
The proposed watermarking system is defined for checking the authentication of color biometric image at the server by proper extraction of watermark. This technique consists of three main phases: watermark embedding, watermark extraction and authentication verification. The steps involved in each phase are as follows:

3.1 Watermark Embedding

The embedding process involves embedding of color watermark image in a color biometric image. The embedding is done invisibly in such a way, that the quality of color biometric image does not degrade much, and the changes done should be imperceptible. The embedding methodology is depicted in Figure 2 and is described as steps as follows:

1. Decompose the color watermark image W into Red (R), Green (G), and Blue (B) channels.
2. Scramble each channel of color watermark image using forward Arnold scrambling to obtain E_R, E_G, and E_B.
3. Decompose cover color biometric image into Red (R), Green (G), and Blue (B) channels.
4. Apply discrete cosine transform on each channel of the cover color biometric image C. Let the coefficients be denoted as D_R, D_G, and D_B, respectively.

Figure 2. Watermark embedding process of proposed technique



5. Apply first level fast discrete curvelet transform (FDCuT) on DCT coefficients of each channel of the cover color biometric image $Cu\left(D_R\right), Cu\left(D_G\right), Cu\left(D_B\right)$.
6. Select a sub band from the FDCuT decomposition according to the size of scrambled color watermark.
7. Embed the scrambled color watermark into cover color biometric image as follows:
   a. Perform SVD on hybrid coefficients (high frequency curvelet coefficients of DCT coefficients) of each channel of cover color biometric image and obtain the corresponding singular (S) matrices:

$$Cu_H\left(D_R\right) = U_R S_R V_R^T \tag{5}$$

$$Cu_H\left(D_G\right) = U_G S_G V_G^T \tag{6}$$

$$Cu_H\left(D_B\right) = U_B S_B V_B^T \tag{7}$$

   b. Save these hybrid Coefficients (S_R, S_G, S_B) of color biometric image for watermark extraction in future.

c. Modify the singular values of cover color biometric image with the scrambled color watermark image as follows:

$$S_R^{'} = S_R + \alpha E_R \tag{8}$$

$$S_G^{'} = S_G + \alpha E_G \tag{9}$$

$$S_B^{'} = S_B + \alpha E_B \tag{10}$$

d. Perform inverse SVD to reconstruct modified hybrid coefficients of cover color biometric image:

$$Cu_H\left(D_R\right)^{'} = U_R S_R^{'} V_R^T \tag{11}$$

$$Cu_H\left(D_G\right)^{'} = U_G S_G^{'} V_G^T \tag{12}$$

$$Cu_H\left(D_B\right)^{'} = U_B S_B^{'} V_B^T \tag{13}$$

8. Apply inverse FDCuT, followed by inverse DCT on modified hybrid coefficients to obtain modified R-G-B channels of cover color biometric image.
9. Perform color image reconstruction from modified R-G-B channels. The result is a watermarked color biometric image.

3.2 Watermark Extraction

The watermark extraction process is depicted in Figure 3 and the details are as follows:

1. Decompose watermarked color biometric image C' into Red (R), Green (G), and Blue (B) channels.
2. Apply discrete cosine transform on each channel of the watermarked color biometric image C' and obtain corresponding DCT Coefficients: D'_R, D'_G, and D'_B.
3. Apply first level fast discrete curvelet transform (FDCuT) on DCT coefficients of each channel of the watermarked color biometric image. Denote them as $Cu\left(D_R\right)^{'}, Cu\left(D_G\right)^{'}, Cu\left(D_B\right)^{'}$.
4. Apply SVD on hybrid coefficients (high frequency curvelet coefficients of DCT coefficients) of each channel of watermarked color biometric image as follows:

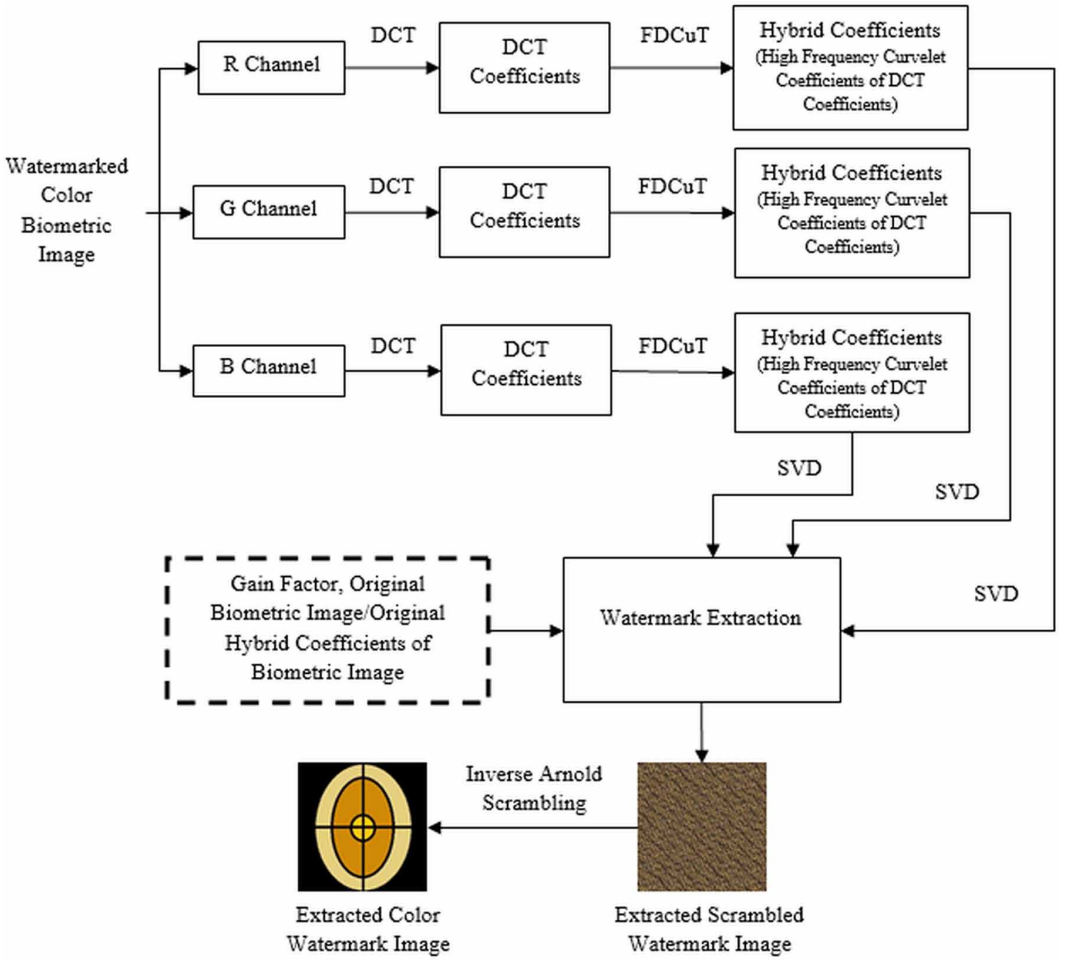
$$Cu_H\left(D_R\right)^{'} = U_R S_R^{''} V_R^T \tag{14}$$

$$Cu_H\left(D_G\right)^{'} = U_G S^{''}{}_G V_G^T \tag{15}$$

$$Cu_H\left(D_B\right)^{'} = U_B S^{''}{}_B V_B^T \tag{16}$$

5. Extract scrambled color watermark image as follows:

Figure 3. Watermark extraction process of proposed technique



$$R_s^{'} = \frac{S_R^{''} - S_R}{\alpha} \tag{17}$$

$$G_s^{'} = \frac{S_G^{''} - S_G}{\alpha} \tag{18}$$

$$B_s^{'} = \frac{S_B^{''} - S_B}{\alpha} \tag{19}$$

where S_R, S_G, and S_B are the hybrid coefficients of original biometric image.

6. Descramble the extracted R-G-B channels using inverse Arnold scrambling to obtain the extracted channels of color watermark image.

7. Perform color image reconstruction using extracted R-G-B channels to obtain the extracted color watermark image *W′*.

3.3 Authentication Process

The proposed scheme performs authentication of biometric image via extraction of color watermark image. The extracted color watermark image is compared with the original watermark image provided by the owner for this purpose. The multi-scale structural similarity index measure (MS-SSIM) (Roy et al., 2014; Wang et al., 2003) is used for comparison watermarks. The comparison value must lie between 0 and 1. Based on the resultant MS-SSIM value and a predefined value τ, two hypotheses are defined for authentication of watermarked color biometric image:

1. If $MS\text{-}SSIM\ (W, W') > \tau$, then consider watermarked color biometric image as authenticated.
2. If $MS\text{-}SSIM\ (W, W') < \tau$, then consider watermarked color biometric image as unauthenticated/ tamper detection

where, W is the original color watermark image and W' is the extracted color watermark image.

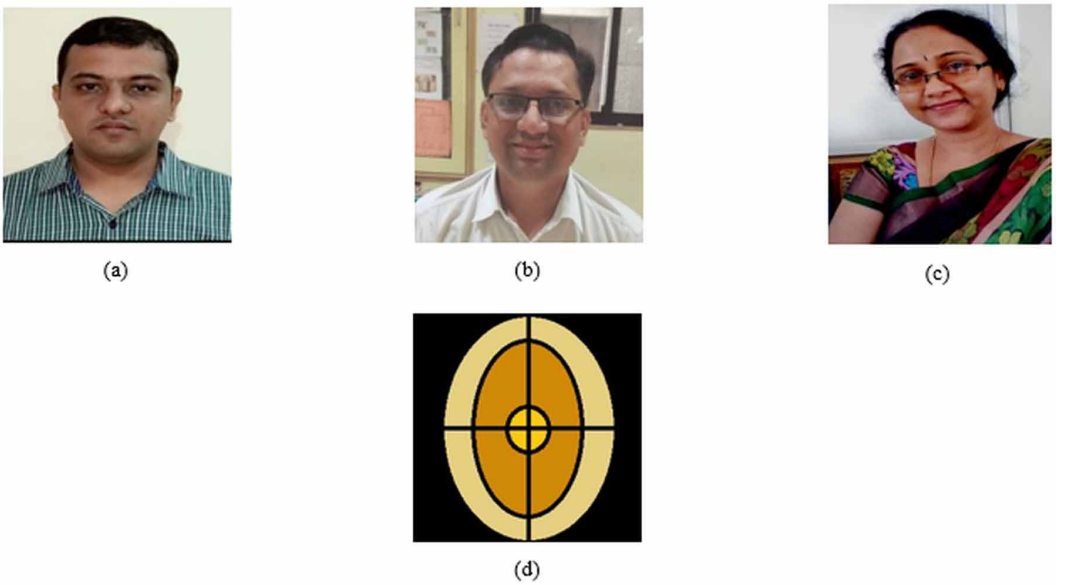
4. RESULTS AND DISCUSSION

The proposed fragile watermarking technique is tested and analyzed by embedding color watermarks in color face biometric images (cover image), both of size 256×256. The test images chosen are shown in Figure 4.

4.1 Performance Measures

The Peak Signal to Noise Ratio (PSNR) (Kutter and Petitcolas, 1999) and weighed PSNR (wPSNR) (Thanki et al., 2018) are used to measure imperceptibility. The PSNR depends on the Mean Square Error (MSE) which is an error between the cover color biometric image and watermarked

Figure 4. Test cover color face images (a) subject 1 (b) subject 2 (c) subject 3 (d) color watermark



color biometric image. The PSNR is measured in dB. Higher the PSNR, higher the invisibility/ imperceptibility, indicating high quality watermarked image. The PSNR is defined as:

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{MSE}\right) \tag{20}$$

The weighted PSNR (wPSNR) is a new approach for calculation of imperceptibility of color biometric images, and is calculated using the equation:

$$wPSNR = 10 \times \log_{10}\left(\frac{255^2}{NVF \times MSE}\right) \tag{21}$$

where, NVF is Noise Visibility Function which gives texture information of biometric image based on the Gaussian model. The value of NVF lies in the interval [0, 1]. The NVF is 0 for texture region and 1 for the flat region. The normalization function, NVF is calculated using the equation:

$$NVF = NORM\left\{\frac{1}{1+\delta^2_{block}}\right\} \tag{22}$$

where δ is luminance variance of computed blocks.

The similarity of the color watermark images is measured by Multi-Scale - Structural Similarity Index Measure (MS-SSIM) (Roy et al., 2014; Wang et al., 2003). The performance of any watermarking technique is high if MS-SSIM is close to 1. The MS-SSIM is defined as:

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)} \tag{23}$$

$$MS - SSIM = \frac{1}{N}\sum_{i=1}^{N} SSIM(x_i - y_i) \tag{24}$$

where, x is the original color watermark image, y is the extracted color watermark image, μ_x is the average of original color watermark image, μ_y is the average of extracted color watermark image, σ_{xy} is the covariance of original color watermark image and extracted color watermark image, C_1, C_2 are constants, and N corresponds to the number of windows.

4.2 Imperceptibility Test

The main requirement of invisible watermarking is that after watermark embedding, the quality of cover image should not degrade, and that the modifications must not be visible to human eye. To test the performance of the proposed technique with respect to this imperceptibility requirement, the watermark shown in Fig. 4d is embedded into three test cover images shown in Fig. 4a-c, using embedding factor α = 0.008, and the results are displayed in Fig. 5. It can be seen that Fig. 5d,

which is a watermarked image, is almost same as Fig. 5a, which is the original image, indicating high imperceptibility. The performance of the proposed watermarking technique is also analyzed objectively, in terms of PSNR, wPSNR and MS-SSIM, and the results are summarized in Table 1, for different gain factors.

Table 1 indicates that for gain factors 0.002 and 0.004, the PSNR is high, indicating high imperceptibility, at gain factor 0.006 and 0.008, the PSNR slides little down, while MS-SSIM remains stable, indicating no difference in structural similarity. The watermarked color face images and extracted color watermark images, for various gain factor values are shown in Figure 6 and 7, respectively. The results indicate that this watermarking technique performs equally well for various gain factors.

The performance of the proposed watermarking technique is also tested on100 color face images, which are taken from FEI Brazilian face database (FEI Face Database, 2009; Thomaz and Giraldi, 2010). The average result of the proposed watermarking technique for this test database, when evaluated at $\alpha = 0.002$, is given in Table 2, which indicates satisfactory results.

Figure 5. (a) Original color face image (b) Original color watermark image (c) Scrambled color watermark image (d) Watermarked color face image (e) Extracted scrambled color watermark image (f) Extracted color watermark image

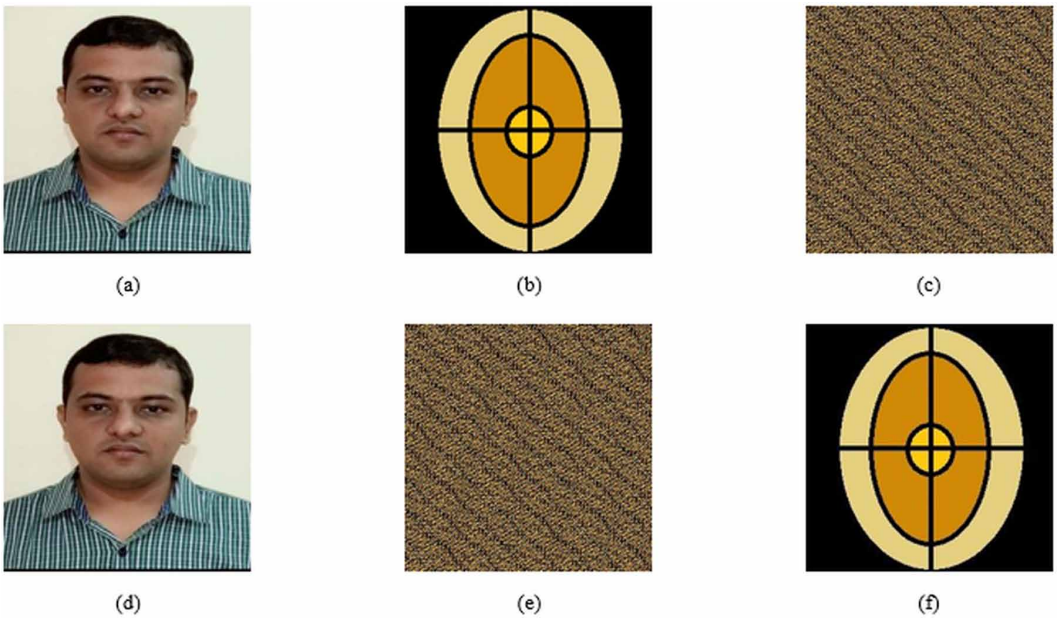


Table 1. Performance of proposed watermarking technique for various gain factors

Test Face Image	$\alpha = 0.002$			$\alpha = 0.004$			$\alpha = 0.006$			$\alpha = 0.008$		
	PSNR (dB)	wPSNR (dB)	MSSSIM	PSNR (dB)	wPSNR (dB)	MSSSIM	PSNR (dB)	wPSNR (dB)	MSSSIM	PSNR (dB)	wPSNR (dB)	MSSSIM
Subject 1	75.66	50.13	1.00	57.92	43.63	1.00	53.14	41.25	1.00	50.72	36.67	1.00
Subject 2	74.09	50.09	1.00	58.15	42.97	1.00	53.45	40.03	1.00	50.98	38.55	1.00
Subject 3	76.46	52.14	1.00	57.76	46.99	1.00	53.05	44.78	1.00	50.57	43.73	1.00

Figure 6. (a) – (c) Watermarked color face image with gain factor value α = 0.002, 0.004 and 0.006



Figure 7. (a) – (c) Extracted color watermark image with gain factor value α = 0.002, 0.004 and 0.006

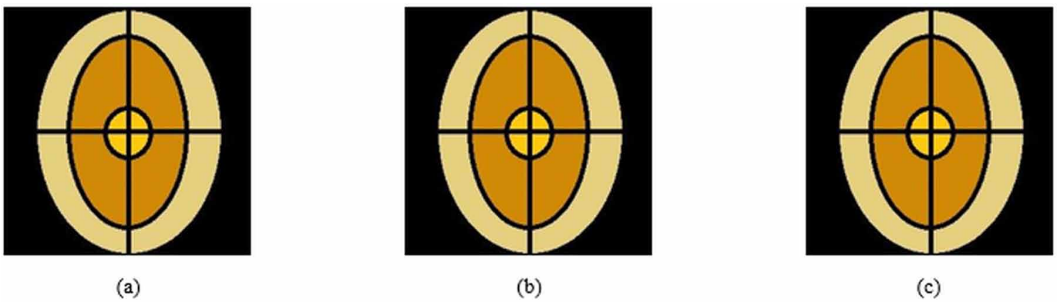


Table 2. Performance of proposed watermarking technique on 100 images

Number of Test Color Face Image in Database	Average PSNR (dB)	Average wPSNR (dB)
100 Face Images	72.86	50.89

4.3 Tamper Detection Test

In the proposed technique, the hybrid high frequency curvelet coefficients of all DCT coefficients are used for watermark embedding, such that, further modifications to the watermarked image, results in loss of watermark, and hence cannot be extracted by watermark extraction algorithm. To test the performance of the proposed technique with respect to tamper detection, the watermarked image is subjected to a variety of attacks, and then fed as input to watermark extraction algorithm. The attacks considered include JPEG compression, addition of different noises, and application of various image filters, histogram equalization, motion blur, and rotation. Figure 8 shows the MS-SSIM values resulted from extraction of watermark for all the three subjects used in the simulations, in the presence of various attacks. The similarity of original and extracted watermarks, being less than 0.15 in Fig.9, indicates loss of watermark in watermarked image, concluding tamper detection. The predefined threshold τ is set to 0.75 in the proposed algorithm. Hence the verification algorithm decides the test image as unauthenticated. The threshold considered here is the standard value reported in the literature (Biometrics and Standards, 2009; Biometrics Testing and Statistics, 2006).

Figure 8. Result of tamper detection test for color face images

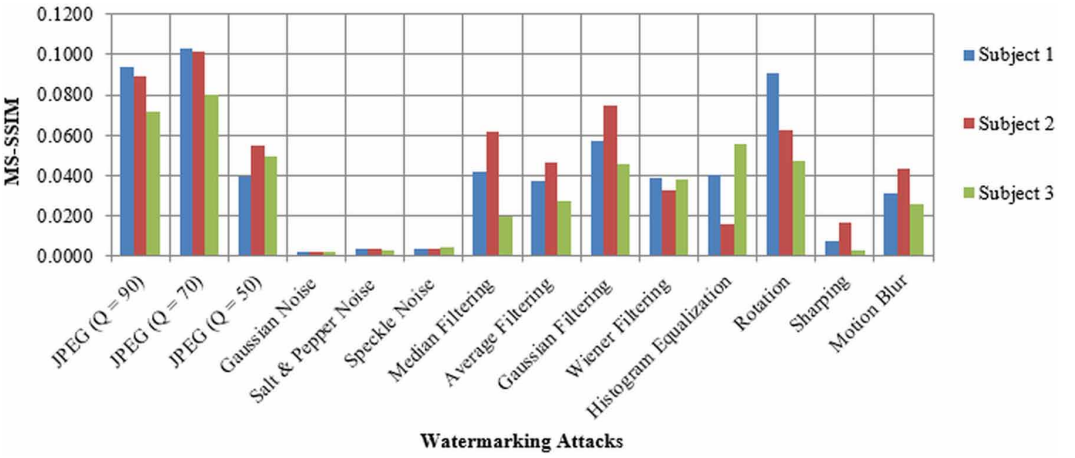
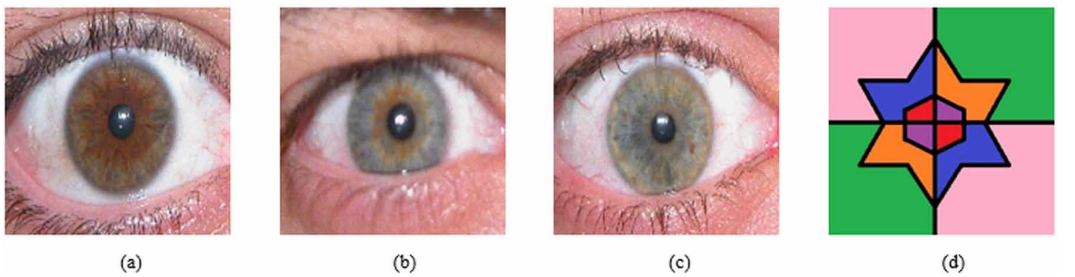


Figure 9. (a) – (c) Original cover color iris image (d) Color watermark image



4.4 Computational Complexity

The computational complexity of watermarking techniques is usually measured in terms of computational time required for watermark embedding process and watermark extraction process. The implementation of the proposed technique is done on the Laptop with 2 GHz i3 processor with 8 GB physical memory using MATLAB 2016b software. The computational time required for watermark embedding and extraction process for three different subjects, under varying gain factors is listed in Table 3. The average computational time for watermark embedding process is 2.7019 s, and extraction process is 2.6411 s, respectively. This indicates that the total computational time for implementation of proposed technique is 5.343s which can be acceptable for any transmission

Table 3. Computational time (s) of proposed watermarking technique for various gain factors

Test Image	$\alpha = 0.002$		$\alpha = 0.004$		$\alpha = 0.006$		$\alpha = 0.008$	
	T_{Embed}	$T_{Extract}$	T_{Embed}	$T_{Extract}$	T_{Embed}	$T_{Extract}$	T_{Embed}	$T_{Extract}$
Subject 1	3.9021	2.7356	2.4434	2.6773	2.6207	2.7876	2.5253	2.5525
Subject 2	2.8015	2.7214	2.6108	2.5713	2.6091	2.5628	2.5544	2.5871
Subject 3	2.5640	2.6599	2.5929	2.5818	2.5434	2.5857	2.6556	2.6702

network. The computational time of the techniques proposed by Joshi et al. (2014) is 6.72 s, Thakkar et al. (2017), is 11.026s, indicating that the proposed scheme is faster.

4.5 Performance of Proposed Technique For Color Iris Image

The performance of the proposed technique is further analyzed using other color biometric images such as iris (shown in Figure 9), which are taken from UBIRIS iris database (Proenca and Alexandre, 2005; Proenca et al., 2010).

Figure 10 (a) and (b) shows the sample1 iris image and color watermark image. The scrambled color watermark image is shown in Figure 10 (c). The watermarked sample 1 iris image and extracted color watermark image using proposed watermarking technique is shown in Figure 10 (d) and 10 (e), respectively. The extracted scrambled color watermark image is shown in Figure 10 (f). By comparing the watermarked image with the original image, it can be concluded that the quality of watermarked image is not degraded, and the modifications are visible. Also using correct key at watermark extraction, a high-quality watermark can be recovered. The PSNR, wPSNR, and MS-SSIM calculated between original and watermarked images for three iris samples are summarized in Table 4.

Figure 11 indicates the MS-SSIM values, computed from original and extracted color watermark images in the presence of attacks. The MS-SSIM values, all being less than 0.13 indicates that when attacks are applied on watermarked color iris images, then the extraction of color watermark image is not possible.

4.6 Authenticity Analysis

In the proposed technique, in order to be properly authenticated, the secret colour watermark should be extracted from the encrypted secret colour biometric image using a secret key *k*. An imposter or attacker cannot extract original watermark, without the private key and hence cannot be authenticated. In the simulation, the secret key *k* is set to 25 for encryption and decryption process. Figure 12 (a) shows decrypted color watermarks with correct secret key *k*. Figure 12 (b) – (d) shows decrypted

Figure 10. (a) Original color iris image (b) Original color watermark image (c) Scrambled color watermark image (d) Watermarked color iris image (e) Extracted scrambled color watermark image (f) Extracted color watermark image

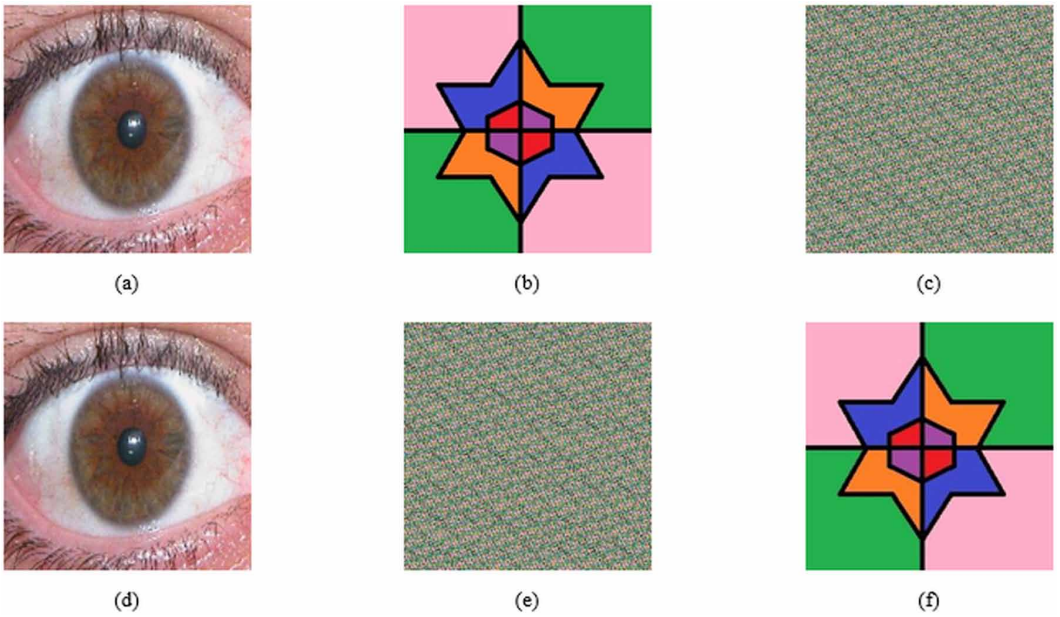


Table 4. Performance of proposed watermarking technique for cover color iris images

Cover Iris Image	$\alpha = 0.002$		
	PSNR (dB)	wPSNR (dB)	MSSSIM
Subject 1	59.47	47.42	1
Subject 2	59.41	48.68	1
Subject 3	59.62	49.80	1

Figure 11. Result of tamper detection test for color iris images

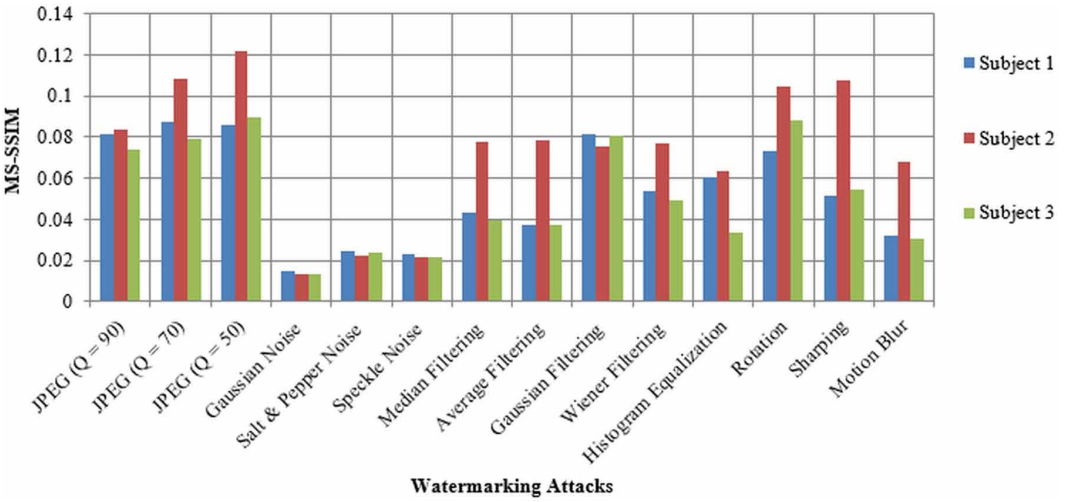
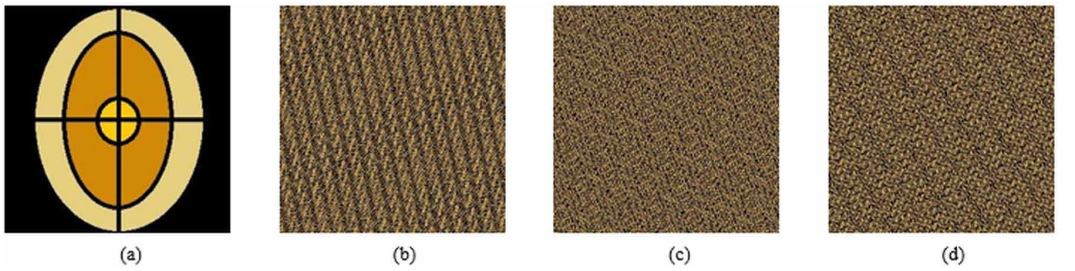


Figure 12. Decrypted secret color watermark image using various keys (a) 25 (b) 5 (c) 15 (d) 35



colour watermarks using wrong secret keys. The results in Fig 12 show that without the correct secret key k, the original watermark cannot be extracted, and hence cannot be authenticated.

4.7 Comparison of Proposed Technique with Existing Techniques

The proposed technique is compared with other similar fragile biometric watermarking techniques with respect to different features in Table 5. The comparison shows that many existing techniques were implemented on grayscale face images, fingerprint image, and iris image. Also, imperceptibility of existing technique in terms of PSNR and watermark size is very low. The proposed technique performed better than many existing techniques in term of imperceptibility and supports large and

Table 5. Comparison of proposed technique with existing fragile biometric techniques

Technique	Watermarking Domain	Used Transform	Type of host image	Size of host image	Encryption of watermark	Application	Maximum PSNR (dB)	Type of Watermark	Size of Watermark
Wang et al. (2008)	Spatial	SVD	Grayscale Iris Image	320×280	Not used	Integrity Verification	Not mentioned	Binary	280 bits
Li et al. (2010)	Spatial	PCA	Grayscale Face Image	128×152	Not used	Tamper Detection and Recovery	Not mentioned	Hash bits	Not mentioned
Yang & Shen (2010)	Spatial	Vector Quantization (VQ)	Grayscale Face Image	256×256	Not used	Tamper Detection	38.15	Binary	256×256
Li et al. (2012)	Spatial	PCA	Grayscale Face Image	128×152	Not used	Tamper Detection and Recovery	43.8	Hash bits	Not mentioned
Li et al. (2013)	Spatial	Not used	Grayscale Fingerprint Image	512×512	Not used	Tamper Detection	54.15	Hash bits	Not mentioned
M. Joshi et al. (2013)	Transform	DWT + SVD and RST	Grayscale Fingerprint Image	320×320	Not used	Image Authentication	47.01	Hash bits	1600 bits
V. Joshi et al. (2013)	Transform	DCT and Vector Quantization	Grayscale Fingerprint Image	320×320	Not used	Image Authentication	44.21	Hash bits	1600 bits
Whitelam et al. (2013)	Spatial	Not used	Color Image	4062×4500	RSA Encryption	Image Authentication	4.5625	Grayscale Face and Fingerprint Image	288*384
Preda (2013)	Transform	DWT	Grayscale Face Image	Not mentioned	Not used	Tamper Detection	66.2	Not mentioned	Not mentioned
Joshi et al. (2014)	Spatial	Not used	Grayscale Fingerprint Image	512×512	RSA Encryption	Image Authentication	51.28	Hash bits	128×152
Joshi et al. (2016)	Hybrid	SVD	Grayscale Fingerprint Image	320×320	Not used	Tamper Detection	48.31	Hash bits	17 bits
Li et al. (2016)	Spatial	SVD and PCA	Grayscale Face Image	768×512	Not used	Tamper Detection and Recovery	53.3	Not mentioned	Not mentioned
Czajka et al. (2016)	Transform	DCT	Grayscale Iris Image	640×480	Not used	Image Authentication	51.35	Hash bits	1024 bits
Tiwari et al. (2017)	Spatial	Vector Quantization (VQ)	Standard Image	256×256	Not used	Image Authentication and Tamper Detection	43.94	Grayscale Fingerprint Image	64×64
Tarif et al. (2017)	Transform	SVD	Color Face Image	640×480	Not used	Tamper Detection	Not mentioned	Not mentioned	Not mentioned
Proposed Scheme	Transform	DCT, FDCuT and SVD	Color Face Image	256×256	Arnold Scrambling	Image Authentication	76.06	Color Image	256×256

color watermarks to be embedded in color biometric images. Further, to meet today's demands, the proposed technique is developed for color face images and color iris images.

5. CONCLUSION AND FUTURE WORK

A color image biometric authentication and tamper detection technique based on non-blind fragile watermarking is proposed in this paper. The hybridization of various transforms such as Discrete Cosine Transform (DCT), Fast Discrete Curvelet Transform (FDCuT), and Singular Value Decomposition (SVD) for watermark embedding resulted in high imperceptibility and high payload capacity, with necessary authentication and tamper detection verification. Further, security of this technique is more as the color watermark is encrypted using Arnold scrambling before its embedding. The proposed

technique is analyzed on FEI Brazilian face database and the performance of the algorithm is evaluated from the biometric image authentication and tamper detection point of view by measuring MS-SSIM in the presence of attacks. Application of this fragile watermarking on biometric images stored at a server or cloud, allows authentication verification and tamper detection when accessed by the remote servers. Apart from supporting large watermarks, the algorithm provided better imperceptibility, authentication and tamper detection, compared to existing watermarking techniques. The limitation of this technique is that it is non-blind and original hybrid coefficients of color biometric image are required in extraction process. The effect of the proposed watermarking technique on the performance of biometric system can be calculated and analyzed in terms of False Rejection Rate (FRR) and False Acceptance Rate (FAR) in the future.

REFERENCES

BBC News Article. (2015, September). *Millions of Fingerprints Stolen in US Government Hack*. Available: https://www.bbc.co.uk/news/technology-34346802

BBC News Article. (2016, April). *Turkish Authorities 'Probing huge ID Data Leak'*. Available: https://www.bbc.co.uk/news/technology-35978216

Biometrics and Standards. (2009, December). *ITU-T Technology Watch Report*. Available: https://www.itu.int/dms_pub/itu-t/oth/23/01/T230100000D0002MSWE.doc

Biometrics Testing and Statistics. (2006, August). *National Science and Technology Council (NSTC) Report*. Available: www.biometrics.gov/documents/biotestingandstats.pdf

Candes, E., Demanet, L., Donoho, D., & Ying, L. (2006). Fast Discrete Curvelet Transforms. *Multiscale Modeling & Simulation*, *5*(3), 861–899. doi:10.1137/05064182X

Candes, E., & Donoho, D. (2004). New Tight Frames of Curvelets and Optimal Representations of Objects with Piecewise-C2 Singularities. *Comm. On Pure and Appl. Mathematics*, *57*(2), 219–226. doi:10.1002/cpa.10116

Czajka, A., Kasprzak, W., & Wilkowski, A. (2016). Verification of iris image authenticity using fragile watermarking. *Bulletin of the Polish Academy of Sciences. Technical Sciences*, *64*(4), 807–819. doi:10.1515/bpasts-2016-0090

Face DatabaseF. E. I. 2006. Available: https://fei.edu.br/~cet/facedatabase.html

Jain, A. (1999). *Fundamentals of Digital Image Processing*. Prentice Hall Inc.

Jain, A., & Kumar, A. (2012). Biometric Recognition: An Overview. In E. Mordini & D. Tzovaras (Eds.), *Second Generation Biometrics, the Ethical, Legal and Social Context* (pp. 49–79). Springer. doi:10.1007/978-94-007-3892-8_3

Jain, A., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, *14*(1), 4–20. doi:10.1109/TCSVT.2003.818349

Jain, A., & Uludag, U. (2002). Hiding Fingerprint Minutiae in Images. In *Proceedings of 3rd Workshop on Automatic Identification Advanced Technologies* (pp. 97-102). Academic Press.

Jain, A., & Uludag, U. (2003a). Multimedia Content Protection via Biometrics-based Encryption. In *Proceedings of IEEE ICME'*03 (pp. III-237). Academic Press.

Jain, A., & Uludag, U. (2003b). Hiding Biometric Data. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *25*(11), 1494–1498. doi:10.1109/TPAMI.2003.1240122

Jain, A., Uludag, U., & Hsu, R. (2002). Hiding a Face in a Fingerprint Image. *Proceedings of IEEE 16th International Conference on Pattern Recognition*, *3*, 756-759. doi:10.1109/ICPR.2002.1048100

Joshi, M. V., Joshi, V. B., & Raval, M. S. (2013). Multilevel semi-fragile watermarking technique for improving biometric fingerprint system security. In *Intelligent interactive technologies and multimedia* (pp. 272–283). Springer. doi:10.1007/978-3-642-37463-0_25

Joshi, V., Raval, M., Rege, P., & Parulkar, S. (2013). Multistage VQ based exact authentication for biometric images. *Computer Society of India (CSI). Journal of Computing*, *2*(1-2), R3–R25.

Joshi, V. B. (2014). Separable Fragile Watermarking for Biometric Image. *PhD Symposium, The 9th Indian Conference on Computer Vision, Graphics and Image Processing (ICVGIP 2014).*

Joshi, V. B., Raval, M. S., Gupta, D., Rege, P. P., & Parulkar, S. K. (2016). A multiple reversible watermarking technique for fingerprint authentication. *Multimedia Systems*, *22*(3), 367–378. doi:10.1007/s00530-015-0465-6

Kutter, M., & Petitcolas, F. A. (1999). Fair benchmark for image watermarking systems. *Security and Watermarking of Multimedia Contents*, *3657*, 226–239. doi:10.1117/12.344672

Leng, L., Zhang, J., Khan, M. K., Chen, X., & Alghathbar, K. (2010). Dynamic weighted discrimination power analysis: A novel approach for face and palmprint recognition in DCT domain. *International Journal of Physical Sciences*, *5*(17), 2543–2554.

Leng, L., Zhang, J., Xu, J., Khan, M. K., & Alghathbar, K. (2010, November). Dynamic weighted discrimination power analysis in DCT domain for face and palmprint recognition. In *Information and Communication Technology Convergence (ICTC), 2010 International Conference on* (pp. 467-471). IEEE. doi:10.1109/ICTC.2010.5674791

Li, C., Ma, B., Wang, Y., & Zhang, Z. (2010, September). Protecting biometric templates using authentication watermarking. In *Pacific-Rim Conference on Multimedia* (pp. 709-718). Springer. doi:10.1007/978-3-642-15702-8_65

Li, C., Wang, Y., Ma, B., & Zhang, Z. (2012). Tamper detection and self-recovery of biometric images using salient region-based authentication watermarking scheme. *Computer Standards & Interfaces*, *34*(4), 367–379. doi:10.1016/j.csi.2012.01.003

Li, C., Wang, Y., Ma, B., & Zhang, Z. (2013). Multi-block dependency based fragile watermarking scheme for fingerprint images protection. *Multimedia Tools and Applications*, *64*(3), 757–776. doi:10.1007/s11042-011-0974-z

Li, C., Yang, R., Liu, Z., Li, J., & Guo, Z. (2016). Semi-fragile self-recoverable watermarking scheme for face image protection. *Computers & Electrical Engineering*, *54*, 484–493. doi:10.1016/j.compeleceng.2016.01.026

Li, M., Liang, T., & He, Y. J. (2013, November). Arnold transform based image scrambling method. *3rd International Conference on Multimedia Technology*.

Nguyen, C., Tay, D., & Deng, G. (2006). A Fast Watermarking System for H.264/AVC Video. In *Asia Specific IEEE Conference on Circuits and Systems* (pp. 81 – 84). IEEE. doi:10.1109/APCCAS.2006.342301

Preda, R. O. (2013). Semi-fragile watermarking for image authentication with sensitive tamper localization in the wavelet domain. *Measurement*, *46*(1), 367–373. doi:10.1016/j.measurement.2012.07.010

Proenca, H., & Alexandre, L. A. (2005, September). UBIRIS: A noisy iris image database. In *International Conference on Image Analysis and Processing* (pp. 970-977). Springer.

Proenca, H., Filipe, S., Santos, R., Oliveira, J., & Alexandre, L. A. (2010). The ubiris. v2: A database of visible wavelength iris images captured on-the-move and at-a-distance. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *32*(8), 1529–1535. doi:10.1109/TPAMI.2009.66 PMID:20558882

Ratha, N., Connell, J., & Bolle, R. (2001). Enhancing Security and Privacy in Biometric Based Authentication Systems. *IBM Systems Journal*, *40*(3), 614–634. doi:10.1147/sj.403.0614

Roy, P., Dutta, S., Dey, N., Dey, G., Chakraborty, S., & Ray, R. (2014, July). Adaptive thresholding: a comparative study. In *Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on* (pp. 1182-1186). IEEE. doi:10.1109/ICCICCT.2014.6993140

Roy, S., & Pal, A. (2017). A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling. *Multimedia Tools and Applications*, *76*(3), 3577–3616. doi:10.1007/s11042-016-3902-4

Surekha, B., Nazare, K. J., Raju, S. V., & Dey, N. (2017). Attendance recording system using partial face recognition algorithm. In *Intelligent techniques in signal processing for multimedia security* (pp. 293–319). Springer. doi:10.1007/978-3-319-44790-2_14

Surekha, B., & Swamy, G. N. (2012). *Digital image ownership verification based on spatial correlation of colors*. Academic Press.

Tarif, E. B., Wibowo, S., Wasimi, S., Tareef, A., & Tareaf, A. (2017, April). A secure hiding scheme for tamper-proofing and authentication of color biometric templates. In *Information and Communication Systems (ICICS), 2017 8th International Conference on* (pp. 141-146). IEEE.

Thakkar, F., & Srivastava, V. (2017). A Fast Watermarking Algorithm with Enhanced Security using Compressive Sensing and Principle Components and its Performance Analysis against a set of Standard Attacks. *Multimedia Tools and Applications*, *76*(14), 15191–15219. doi:10.1007/s11042-016-3744-0

Thanki, R., & Borisagar, K. (2014, October). Security of biometric data using compressed watermarking technique. *Iranian Journal of Electrical and Computer Engineering*, *4*(5), 758–766. doi:10.11591/ijece.v4i5.6646

Thanki, R., Borra, S., Dey, N., & Ashour, A. S. (2018). Medical Imaging and Its Objective Quality Assessment: An Introduction. In *Classification in BioApps* (pp. 3–32). Springer. doi:10.1007/978-3-319-65981-7_1

The Hindu Business Line Article. (2017, May). *Aadhaar Data Leak Exposes Cyber Security Flaws*. Available: https://www.thehindubusinessline.com/info-tech/aadhaar-data-leak-exposes-cyber-securityflaws/article9677360.ece

Thomaz, C., & Giraldi, G. (2010). A New Ranking Method for Principal Components Analysis and its Application to Face. *Image and Vision Computing*, *28*(6), 902–913. doi:10.1016/j.imavis.2009.11.005

Tiwari, A., Sharma, M., & Tamrakar, R. K. (2017). Watermarking based image authentication and tamper detection algorithm using vector quantization approach. *AEÜ. International Journal of Electronics and Communications*, *78*, 114–123. doi:10.1016/j.aeue.2017.05.027

Unique Identification Authority of India. (2016). *Operation Model*. Available: https://www.uidai.gov.in/authentication/authentication-overview/operation-model.html

Vidyasree, P., Madhavi, G., Viswanadharaju, S., & Borra, S. (2018). A Bio-application for Accident Victim Identification Using Biometrics. In *Classification in BioApps* (pp. 407–447). Springer. doi:10.1007/978-3-319-65981-7_15

Wang, D. S., Li, J. P., & Wen, X. Y. (2008, May). *Biometric image integrity authentication based on SVD and fragile watermarking. In 2008 Congress on Image and Signal Processing*. IEEE.

Wang, Z., Simoncelli, E., & Zhang, D. (2003). Multi-scale Structural Similarity for Image Quality Assessment. *Proceedings of the 37th IEEE Asilomar Conference on Signals, Systems and Computer*.

Whitelam, C., Osia, N., & Bourlai, T. (2013, November). Securing multimodal biometric data through watermarking and steganography. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on* (pp. 61-66). IEEE. doi:10.1109/THS.2013.6698977

Wong, P. W., & Memon, N. (2001). Secret and public key image watermarking schemes for image authentication and ownership verification. *IEEE Transactions on Image Processing*, *10*(10), 1593–1601. doi:10.1109/83.951543 PMID:18255501

Yang, C. W., & Shen, J. J. (2010). Recover the tampered image based on VQ indexing. *Signal Processing*, *90*(1), 331–343. doi:10.1016/j.sigpro.2009.07.007

Rohit Thanki is a computer vision expert and AI researcher with more than 5 years of work experience in areas of computer vision, medical image analysis & security, artificial intelligence and biometrics including 2 years of academic experience in various engineering institutions in India. Presently, he is working as a research & development director, Prognica Labs Tech FZCO, Dubai, UAE. He earned his bachelors in electronics & communication, master's in communication engineering and a doctorate degree in electronics & communication with a specialization in digital image processing and biometric security. His areas of research interest are medical image analysis, artificial intelligence, machine learning, deep learning, digital watermarking, biometric security, compressive sensing, and signal processing. He has more than 40 publications in his credit and has published in reputed journals with high impact factor and international conferences indexing in Scopus / SCIE / WOS. Also, He has authored and contributed more than 20 books with reputed publishers, i.e., Springer, CRC press, Elsevier, De Gruyter, and IGI Global. He has been invited as reviewer in various reputed journals such as ACM Transactions on Multimedia Computing, Communications and Applications, IEEE Consumer Electronics Magazine, IEEE Access, IEEE Journal of Biomedical and Health Informatics, Signal Processing: Image Communication, Pattern Recognition, Computers and Electrical Engineering, Informatics in Medicine, Journal of Ambient Intelligence and Humanized Computing, IET Biometrics, and IET Image Processing.

Surekha Borra is currently a Professor in the Department of ECE, K. S. Institute of Technology, Bangalore, Karnataka, India. She earned her Doctorate in Image Processing from Jawaharlal Nehru Technological University, Hyderabad, India, in 2015. Her research interests are in the areas of Image and Video Analytics, Machine Learning, Biometrics and Remote Sensing. She has published 2 Books, 10 book chapters and 30 research papers to her credit in refereed & indexed journals, and conferences at international and national levels. Her international recognition includes her professional memberships & services in refereed organizations, programme committees, editorial & review boards, wherein she has been a guest editor for 2 journals and reviewer for journals published by IEEE, IET, Elsevier, Taylor & Francis, Springer, IGI-Global etc. She has received Woman Achiever's Award from The Institution of Engineers (India), for her prominent research and innovative contribution (s)., Distinguished Educator & Scholar Award for her contributions to teaching and scholarly activities, Young Woman Achiever Award for her contribution in Copyright Protection of Images.

Ashish M. Kothari obtained his Ph.D. in Digital Video Watermarking from JJT University, Rajasthan, India in 2013. He is working as an Associate professor and Head of Electronics and Communication Engineering, Atmiya Institute of Technology and Science, Rajkot, Gujarat, India. He is also recognized Ph.D. supervisor at Gujarat Technological University, Ahmedabad, Gujarat, India. His area of research interest is Image Processing, Video Processing, Digital Watermarking and Signal Processing. He has published 2 book, 1 book chapters and more than 25 research papers to his credit in refereed & indexed journals, and conferences at international and national level.