STUDY OF SECURE BIOMETRIC AUTHENTICATION SYSTEM FOR REVERSIBLE DATA HIDING USING STEGANOGRAPHY

Ms. S. Selvarani[1]*, Dr. M. Mary Shanthi Rani[2]

Abstract

In all smart environments, biometric authentication is utilised to the utmost extent possible. The two most common methods for biometric authentication are face and fingerprint recognition. The combination of face recognition and fingerprint recognition can be installed in specific locations where a higher level of security is necessary. Typically, a camera and fingerprint scanner will be used to gather biometric data on the client side, and that data will then be sent to a Cloud Service Provider (CSP) to perform complicated tasks like face and fingerprint identification. In these circumstances, the transmission of facial photos and fingerprints from the client side to a server is a significant security risk since a hacker could attempt to steal that information and then use it to take over the authentication system. In this research work, a secure method for transmitting fingerprints and face photos using an encryption strategy that uses Reversible Data Hiding (RDH) is used. RDH is a technique for concealing information by employing a medium that makes it feasible to later recover the original images as well as the concealed message. To conceal the secret message in an image, an RDH via encryption strategy will combine the RDH process and the image encryption process into a single job. In this research paper, a new paradigm is suggested in which the compressed fingerprint data will be integrated into the facial image as a secret message using a Reversible Data Hiding technique. After RDH, the encrypted image that was obtained will be sent for additional processing to the cloud service provider.

Keywords: Cloud Service Provider, Reversible Data Hiding, Watermarking, Steganography

[1]*M.C.A., M.Phil.,(Ph.D.,) Assistant Professor, Department Of Computer Applications, Fatima College, Mary Land, Madurai. Email: Rani.S.Selva@Gmail.Com
[2]Research Supervisor, Associate Professor, Department Of Computer Science & Applications, The Gandhigram Rural Institute (Deemed To Be University), Dindigul. Email: Drmaryshanthi@Gmail.Com

***Correspondence Author:** Ms. S. Selvarani
*****M.C.A., M.Phil.,(Ph.D.,) Assistant Professor, Department Of Computer Applications, Fatima College, Mary Land, Madurai. Email: Rani.S.Selva@Gmail.Com

DOI: - 10.48047/ecb/2023.12.si5a.0146

I. INTRODUCTION

Digital imaging and communication technologies have recently been used to disseminate and distribute digital information via open networks, offering a crucial and efficient technique in a variety of applications [1]. Electronic health, copyright protection, secures information in cloud and dispersed contexts, fingerprinting, distance learning, etc. are all included in the programme. A high level of security and privacy is still necessary for the transmission, storage, and sharing of sensitive information through unsecure communication networks [2, 3]. Sensitive data and information can be protected with high levels of secrecy, integrity, availability, and authenticity using watermarking and encryption techniques. Other benefits of prospective watermarking approaches include ownership identification, avoiding detaching, protection against tampering, access control, non-repudiation, indexing and efficient archiving, and lowering memory and bandwidth requirements [2, 4].

II. PROCESS FOR EMBEDDING AND EXTRACTING WATERMARKS.

The key distinctions between watermarking and other comparable security measures are shown in Table 1 [5, 6]. Watermarking methods are either spatially or trans formatively domain-specific. The study came to the conclusion that transform-based techniques are more reliable than spatial domain watermarking methods including LSB, patch work, correlation-based, and spread spectrum. Some potential examples of trans form based approaches are DWT, SVD, DCT, DFT, and KLT [7]. The embedding and extraction of the watermark are depicted in Figure 1(a)-(b)

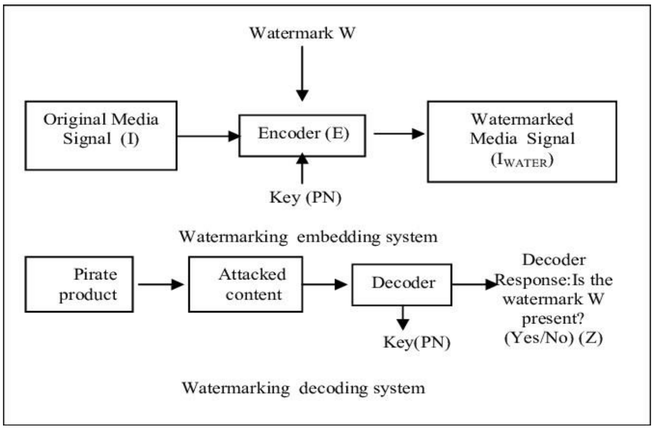
Watermark W
Original Media Signal (I)
Encoder (E)
Watermarked Media Signal (I_{WATER})
Key (PN)
Watermarking embedding system
Pirate product
Attacked content
Decoder
Decoder Response:Is the watermark W present? (Yes/No) (Z)
Key(PN)
Watermarking decoding system

Fig. 1 watermarking (a) embedding and (b) decoding process

The cover, watermark, and optional secure key all work together to create the watermark embedding process. The watermarked image is the result of the embedding procedure. The role of the watermarked image/cover data, optional secure key, and test data is the watermark extraction method [7]. Most prospective authors now use both objective and subjective evaluation techniques to assess the effectiveness of any watermarking technology. The accurate value is based on mathematical modelling that represents the visual quality of the digital image, and is determined by objective evaluation techniques including Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), and Just Noticeable Difference (JND) [4]. By capturing human subjects' opinions based on the apparent visual quality, subjective assessment techniques are used to measure the visual quality.

Table 1. The Difference between Watermarking and Comparable Security Measures

Property	**Water marking**	**Cryptography**	**Steganography**	**Finger printing**	**Digital Signat**
Definition	Watermark ing is the process of adding a mark to any image,	Cryptography is used to secure the digital data by	Steganography is used to hide the data in such a	Fingerprinting is a technique which takes a	**ultre** is a technique for verifying the accura
Secret data and key	Watermark is embedded In multimedia file	Encryption and decryption process are	Payload is embedded in any digital media with an optional key and used to hide	It is uniquely identified to secure the data	It is used for authenticity of
Selection of cover	Restriction in cover image	used some secret key	The message It is a	Cover selection	Digital documents
Attacks	Active, Passive,	Side-Channel	Brute force	Traffic fingerprint	Birthday
Type of communication	One- to- many communications	Probing attacks One- to- many	One- to- one	One-to- many	One- to-one

III. FUNDAMENTAL TRAITS OF DIGITAL WATERMARKS

The fundamental properties of watermarks include robustness, security, data payload, imperceptibility, fragility, embedding capacity, computational cost, and key constraints [7, 8]. The fundamental attributes of digital watermarks are displayed in Fig. 2.

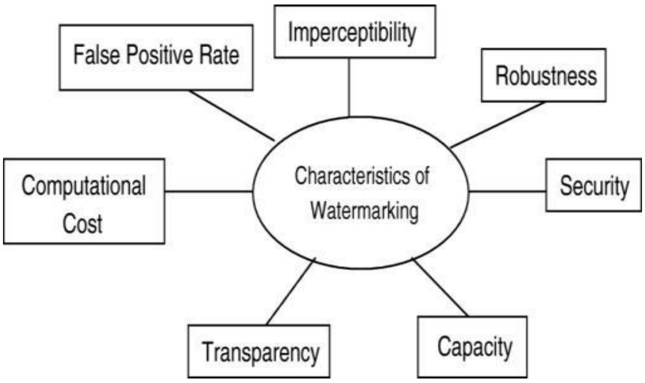

Fig. 2 Characteristics of digital watermarks

Also, the key uses that match the fundamental characteristics of the watermark was determined.

Table 2 provides a summary of the key attributes and associated uses of digital watermarks.

Basic Characteristics	Definition	Applications
Robustness	Recovery of embedded data against attacks. Focus on copyright protection	Copyright protection, Forensic applications, Digital Imaging processing, graphics, telemedicine etc
Security	Watermark should be hard to alter OR remove without harming the cover image.	Telemedicine, Military, Multimedia, Digital Imaging, Tele-communication, ownership proof, fingerprinting etc.
Data Payload	It depends upon the total amount of the information that it contains	Video, Network based Communication, Digital Imaging, Computer Chip Hardware etc
Imperceptibility	It show the imperceptibly embed the watermark without degradation of the cover.	Digital Imaging, telemedicine, Digital Documents, claim of ownership, Network patrolling, Meta level etc.
Fragility	Focus on content authentication	E- governance, Law enforcement, digital signal, defence, commerce, journalism, telemedicine etc.

IV MODERN USES FOR DIGITAL WATER MARKING

For several new applications, potential researchers are employing watermarking techniques. The application includes network flow watermarking, watermarking in distributed cloud computing environments, and big data watermarking [3, 7]. It also includes hardware and chip level security, copyright protection, electronic voting, audio/video, robotics, remote education, digital forensic, military, broadcast monitoring, and media security solutions in smart cities. Fig. 3 shows a recent example of digital watermarking in use.

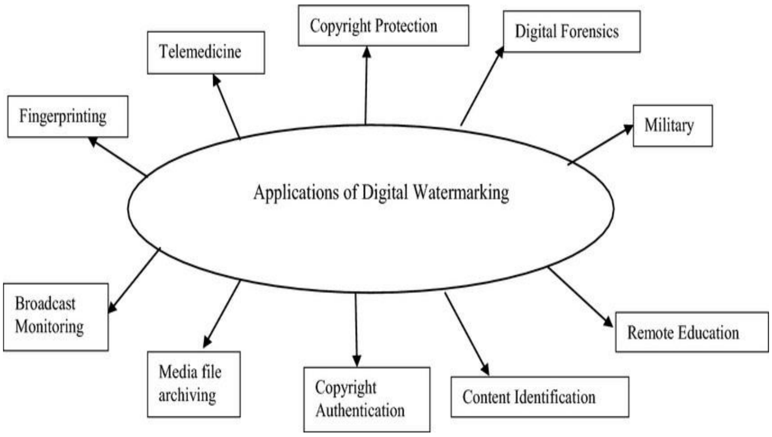

Fig. 3 Application of digital watermarking

V. CLASSIFICATION OF WATERMARKING ATTACKS

Knowledge of watermarking systems is necessary to classify watermarking assaults [9]. System assaults and attacks targeted to unauthorised actions are two major categories for the attacks. System assaults are caused by the incorrect use of watermarks. Whereas exploiting watermarks' flaws results in unlawful action, such as targeted attacks. Fig. 4 [9] depicts a classification of watermarking attacks.

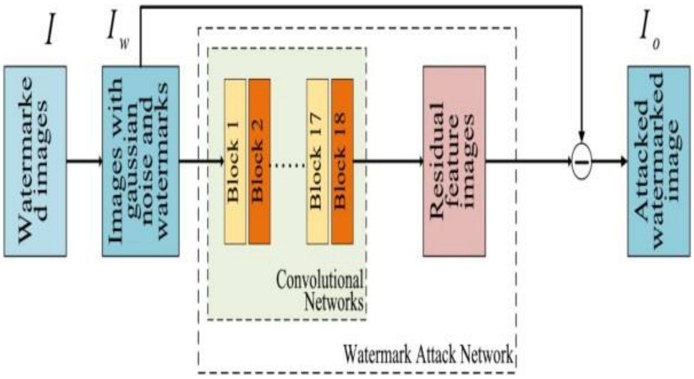

Fig. 4 Important attacks of watermarking technique

VI LITERATURE REVIEW

The primary performance criteria for watermarking systems include robustness, imperceptibility, capacity security, and computational complexity. With any given watermarking algorithm, it can be challenging to keep these parameters in balance. Secure watermarking systems can be achieved using crypto graphy, chaotic logistic map (s), hashing, spread spectrum, biometric, fingerprinting, Hessen berg matrix, digital signature, etc., Through the use of visual cryptography, chaotic logistic map(s), hashing, spread spectrum, elliptical curve cryptography, Chinese remainder theorem, biometrics, digital fingerprinting, homomorphic cryptosystem, Hessen berg matrix, and digital signature, as shown in Fig. 5, potential researchers and authors who have developed secure watermarking was identified.

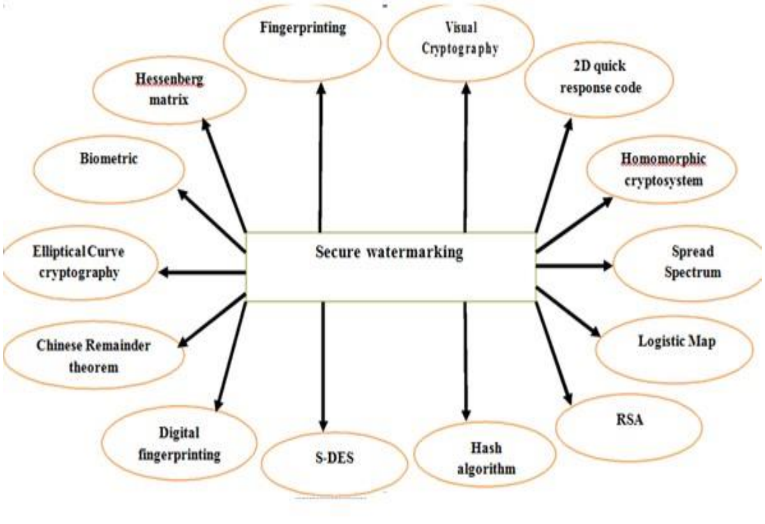

Fig. 5 Secure watermarking through different techniques

The authors of [8, 10, 13] devised a watermarking methodology using the logistic map technique to ensure the integrity and validity of the outsourced data.

[12] introduces a blind colour image watermarking technique. The programme blindly extracts the watermark using a key-based quantization. Also, the spatial domain technique is straightforward and increases the watermarking method's robustness and imperceptibility using DCT.

The homomorphic cryptosystem is used by the method in [3, 12] to ensure the security of the watermarking system. Moreover, the combination of DWT-DCT improves the method's resilience. The watermarking method used in [7, 12] makes advantage of compression techniques to offer a good embedding capacity for real-world applications. Moreover, the AMBTC-based water marking approach [7] requires less computing effort. Authors in [13] are given patient identity/ information security via a watermarking technique in a framework for IoT-enabled health monitoring. Also, combining two well-known transform techniques will increase the system's robustness.

In [11], 2D rapid response code is used to provide patient information security. Moreover, the system's resilience is increased by merging two transform domain techniques. In [15], visual cryptography with an adaptive order dithering methodology is used to provide the security of the watermarking method.

The Arnold and MD5-based Hash pseudo-random algorithms used in [7] make the proposed system secure and reliable, respectively. According to [16], elliptical curve cryptography is used to secure the system. Also, compared to RSA and Direct Selling Association encryption methods, the ECC-based solution is quicker.

In recent years, there has been a lot of research on digital watermarking, also known as water marking, which is described as embedding information about the origin, destination, access level, etc. of multimedia data (such as image, video, audio, etc.) in the host data [17]. Depending on the area in which watermarking is used; general image watermarking techniques can be separated into two categories. Changes are made to the pixel values in the picture channel(s) in spatial domain algorithms (such as [7]). A watermark signal is introduced to the host image in spectral-transform domain techniques in a transform domain like the full-frame DCT domain [8].

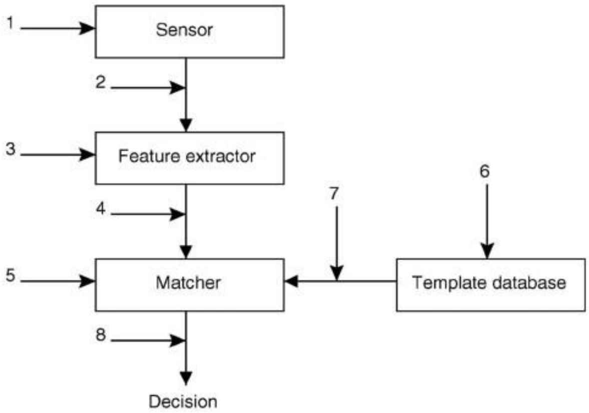

Fig 6. Different attack points in a biometric authentication system

Only a small number of publications on fingerprint image watermarking have been published. A data hiding technique was put out by Ratha et al. [9] and is applicable to fingerprint images compressed using the WSQ wavelet-based methodology. During WSQ encoding, the discrete wavelet transform coefficients are modified to account for potential image degradation. A fragile water marking method for fingerprint image verification was put out by Pankanti and Yeung [10]. A verification key is used to incorporate a spatial watermark image in a fingerprint image's spatial domain. Every altered area of an image can be localised using the suggested method. According to Pankanti and Yeung, fingerprint verification does not significantly suffer from the use of their watermarking technology. Jain [11] uses a semi-unique key based on local block averages to identify fingerprints and faces in host images that have been altered. Two spatial domain water marking techniques for fingerprint photographs were presented by Gunsel et al. [12]. The first technique applies gradient orientation analysis to watermark embedding, ensuring that none of the characteristics retrieved from gradient information are changed during watermarking. The classification of the watermarked fingerprint image (e.g., into arch, left loop, etc.) is unaffected by the second approach since it preserves the unique points in the fingerprint image.

VII HIDING BIOMETRIC DATA

In this study, two application situations are taken into account. Although the underlying data concealing technique is the same in both cases, there are differences in the features of the embedded data, the host picture that contains that data, and the media used for data transfer. While face and fingerprint feature vectors as the embedded data, other data, such a user name or user identification number, can also be concealed in the photos. To improve the system's overall security, it was chosen to safeguard one form of biometric data using another type of biometric data.

(A) APPLICATION SCENARIOS

Water marking based application is used in the first situation (figure.1) The host (also known as cover and carrier) image's sole purpose is to transport the biometric data (fingerprint minutiae) that must be communicated (potentially via an insecure communication channel). For instance, the transmission of fingerprint details from a law enforcement agency to a template database, or vice versa, may be necessary. In this case, the system's security is predicated on the communication's confidentiality. The host picture has nothing to do with the concealed data at all. The host image can therefore be any image that the encoder has access to. In this programme, three different kinds of cover images were taken into account: a fake fingerprint, a fake face, and a random image (Fig. 8). The image created by the technique described by Cappelli et al. [13] is post processed to produce the synthetic fingerprint image (360 x 280). Since the person who intercepts the communication channel and acquires the carrier image is likely to mistake this synthetic image for a real fingerprint image, using it to convey true fingerprint minutiae data offers a higher level of Security.

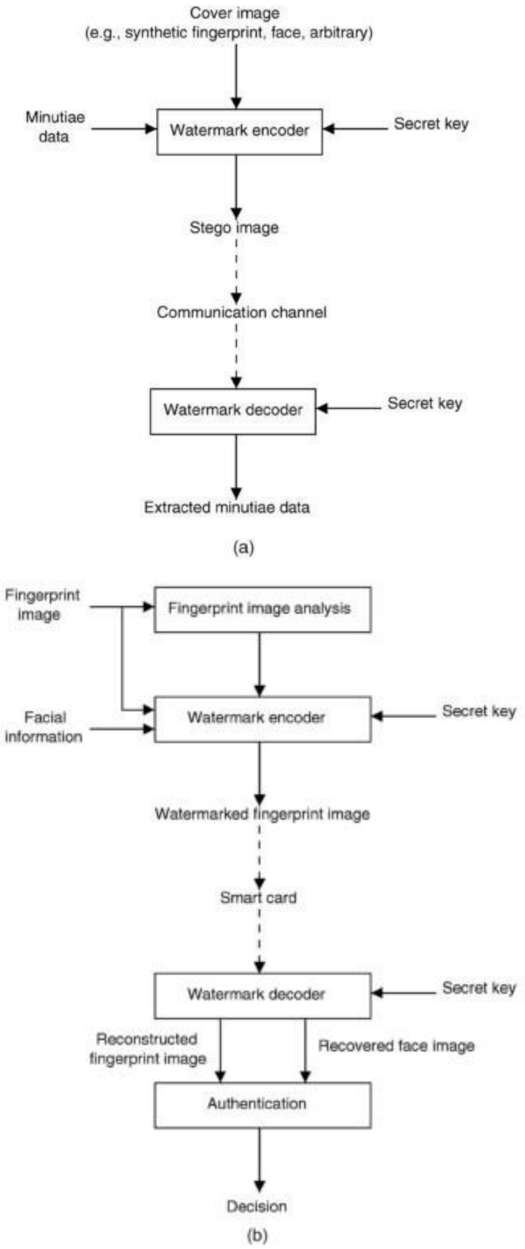

Fig 7(a, b). Diagrams of application scenarios (a) Cover image (b) fingerprint image

The blue channel watermarking approach of Kutter et al. [7] is extended in the amplitude modulation based watermarking method that is given here. Together with the fundamental method in [7], the suggested method also takes into account picture adaptivity, a watermark strength controller, and host image feature analysis. A previous iteration of the method is provided in [12], which analyses the improvement in data decoding accuracy brought on by these improvements. The data that will be concealed within the host image is first converted to a binary stream. Every field of each individual fingerprint minutia is converted to a 9-bit binary representation in the first scenario, when fingerprint minutiae data are hidden. Such a model is capable of encoding numbers in the range [0, 511], which is suitable for representing a minutia's x-coordinate ([0, N-1]), y-coordinate ([0, M-1]), and orientation ([0, 359]), where N and M are denotes the fingerprint image's number of rows and columns, respectively.

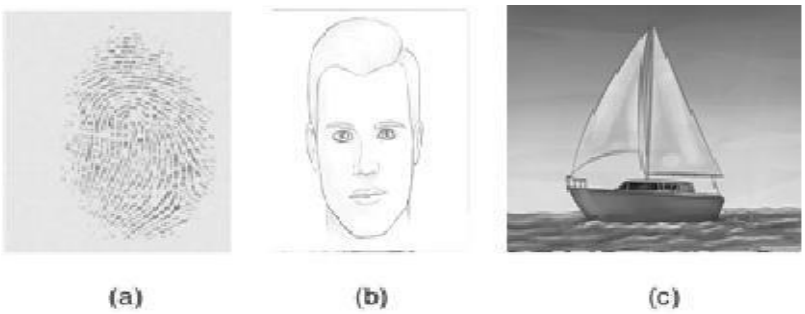

Fig. 8. Sample cover images: (a) synthetic fingerprint, (b) face, and (c) “Sailboat.”

In the second situation, four bytes are used to turn each eigen-face coefficient into a binary stream. The positions of the host picture pixels that will be watermarked are generated by a random number generator that is initialised with the secret key. Here are the specifics of this process: Then, a uniform distribution is used to create a series of random values between 0 and 1. Then, every integer with an odd index is linearly mapped to [0, X-1] and every number with an even index is linearly mapped to [0, Y-1], where X and Y are the host image's row and column counts, respectively. Every pair that contains one number with odd indices and one number with even indices points to a potential pixel that has to be tagged. A pixel should not be modified more than once during the watermark embedding process as this could result in improper bit decoding. Moreover, there is no marking on the pixels if (i,j)th (marked pixel map, detailed below) is zero. The next pixel location is taken into consideration if, at any point during embedding, the candidate pixel cannot be marked because of one of these circumstances. The pixel at (i,j) is modified using the following equation.

$$P_{WM}(i,j) = P(i,j) + (2s-1)P_{AV}(i,j)q \\ * \left(1+\frac{P_{SD}(i,j)}{A}\right)\left(1+\frac{P_{GM}(i,j)}{B}\right)\beta(i,j), \qquad (1)$$

where $P_{WM}(i,j)$ and $P(i,j)$ represent, respectively, the values of the watermarked and original pixels at location (i,j). The value of the watermark bit is denoted as s, and the degree of embedding is denoted as q, where s [0,1] and q > 0. P_{GM} (i j) specifies the gradient magnitude at pixel (i,j), while $P_{AV}(i,j)$ and $P_{SD}(i,j)$ denote the average and standard deviation of pixel values in the area around pixel (i,j) (i,j). Standard deviation and gradient magnitude are weighted by the parameters A and B, which modulate the effects of these two terms. Increasing either of these parameters reduces the overall modulation effect on the amount of change in pixel intensity, while decreasing either one has the opposite effect. The minimum values of P_{SD} (i,j) and P_{GM} (i,j) are both 0, corresponding to neighbourhoods with constant grey levels; the maximum value of P_{SD} (i,j) is around 127, corresponding to a checkerboard-style pixel pattern with only 0 and 255 grey levels. A maximum magnitude diagonal edge has a maximum value for P_{GM} (i,j) of about 1,082. (e.g., intersection of grey levels 0 and 255). The (i,j) term ensures that image pixels, referred to as marked pixels, whose change may affect the effectiveness of an algorithm using the watermarked image (for example, fingerprint verification in the case of watermarked fingerprint images), remain unchanged. (i,j) takes the value 0 if the pixel (i,j) is a marked pixel and the value 1 otherwise. These three factors P_{SD} (i,j), P_{GM} (i,j), and (i,j) significantly modify the fundamental marking method described in [7] by modulating the amount of change in pixel values brought about by marking.

In the second situation, either ridge analysis or minutiae analysis of the fingerprint image is used to determine the indicated pixels. In the tests, P_{SD} is calculated in a neighbourhood that is 5 x 5 cross-shaped, while P_{AV} is calculated in a neighbourhood that is 5 x 5 square. The 3 x 3 Sobel operators are used to calculate the gradient magnitude.

By exploiting a number of features of the human visual system, the images presented above modify the level of watermarking (HVS). Using P_{AV} (*i,j*) to modulate watermark magnitude complies with HVS's amplitude nonlinearity. As seen in (1), when the P_{AV} (*i,j*) value is high, watermarking causes a larger change in the value of pixel (*i,j*) than when it is low. Standard deviation and gradient magnitude terms make use of the HVS's contrast/ texture masking capabilities. These picture adaptivity parameters enhance the amount of watermarking in sections of the image where a human observer would not be able to see the increase very well.

Each watermark bit with a value of s in (1) is inserted in the host picture several times. The accurate decoding rate of the embedded information is accelerated by this redundancy. The image capacity (size) and visibility of the changes in pixel values set a limit on the quantity of this redundancy. Moreover, the *(i,j)* mask keeps important aspects of the host fingerprint image. The host image additionally contains two reference bits, numbered 0 and 1, in addition to the binary watermark data. As the watermark bit values are being decoded, these reference bits aid in the calculation of an adaptive threshold. The secret key used during the watermark encoding stage is utilised to locate the data embedding sites in the watermarked image to begin the decoding process. It should be noted that only the watermarked image is used for decoding; the original, non-water marked image is not.

The linear combination of pixel values in a 5 x 5 cross-shaped neighbourhood around the water marked pixels are used to estimate each bit embedding location's value during decoding (2) calculated as A(14,100) and B(14,1000), the difference between estimated and watermarked pixel values. The buried data becomes more obvious as the q value rises. Standard deviation and gradient magnitude have less of an impact on altering the strength of the watermark when A or B are increased, respectively.

The hidden data in this case is about 85 bytes big. It is discovered that the concealed data and the retrieved minutiae data from each of the three cover images are identical. Also, the following criteria were used to assess the performance of the suggested algorithm: 15 photos (five arbitrary, five face, and five synthetic fingerprints) were water marked with five separate sets of minute data and five different keys. The consequence was the creation of v1Different watermarked photos. The host photos' characteristics, sources, and water marking parameters are the same as before. With an average of 25, individual minutiae data sets ranged from 23 to 28 points. There was 100% accuracy in the ability to retrieve the underlying minutiae data from all 375 watermarked photographs.

$$\hat{P}(i,j) = \frac{1}{8}\left(\sum_{k=-2}^{2} P_{WM}(i+k,j) + \sum_{k=-2}^{2} P_{WM}(i,j+k) - 2P_{WM}(i,j)\right). \quad (2)$$

The difference between the estimated and watermarked pixel values is calculated as

$$\delta = P_{WM}(i,j) - \hat{P}(i,j). \quad (3)$$

These discrepancies are averaged across all embedding locations linked to the same bit to produce. These averages are generated individually for the reference bits, 0, and 1, as R0 and R1, respectively, to determine an adaptive threshold. The watermark bit value s is finally estimated to be.

$$\hat{s} = \begin{cases} 1 & \text{if } \bar{\delta} > \frac{\bar{\delta}_{R0}+\bar{\delta}_{R1}}{2}, \\ 0 & \text{otherwise.} \end{cases} \quad (4)$$

In the second application scenario, the input face image (150 x 130) is used to watermark the fingerprint image (300 x 300) displayed in Fig. 10 a. The 14 eigen-face coefficients, or 56 bytes, that makes up the watermark information (four bytes per coefficient). The 150 x 130 watermark face image of Fig. 10 c is produced by these 14 eigen-face coefficients [17].

It should be noted that a high-fidelity reconstruction of the input face can be achieved with just 14 eigen-face coefficients. The eigen-faces and coefficients were generated using a tiny face picture collection that has 40 photos total—four images for each of the 10 individuals.

Figures 10d and 10e correspond to data concealing based on minute details. Without altering the pixels 0, the input image in Fig. 10a is watermarked:

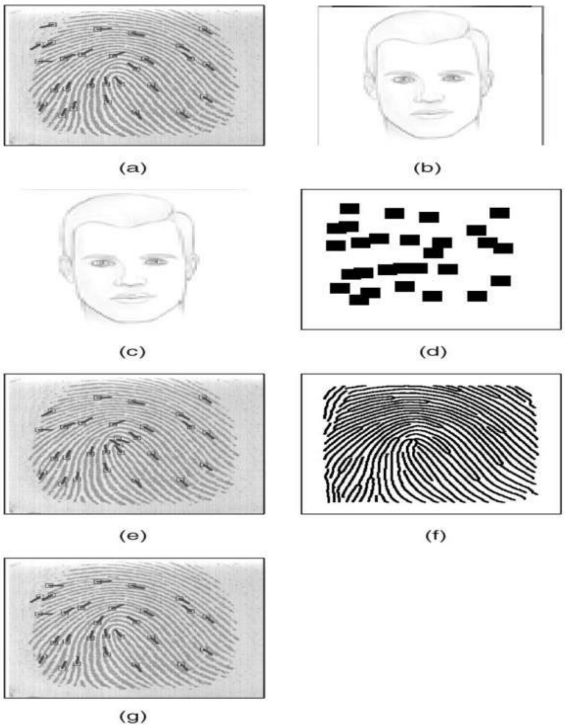

Fig. 10. Facial information embedding and decoding: (a) input fingerprint image with overlaid minutiae; (b) input face image; (c) watermark face image; (d) fingerprint feature image based on minutiae; (e) reconstructed fingerprint image with overlaid minutiae; (f) fingerprint feature image based on ridges; I reconstructed fingerprint image with overlaid minutiae; where watermarking did not change the pixels shown in black (f).

Equation (4) effectively states that a bit is declared to be "1" if it is closer to R1 than R0, and "0" if it is closer to R1 than R0. As the watermark decoding method relies on an estimating procedure that might not be able to determine the precise original pixel values, it may result in erroneous bits. This could result in decoding having swapped bits.

Additionally, embedding crucial information was embedded, where even a single bit alteration can make the data less usable, every embedded bit in this work should be successfully decoded (i.e., a 0% error rate) (e.g., minutiae data change, eigen-face coefficient changes due to switched bits). The encoder uses a controller block to improve the decoding precision. If there is a chance of improper bit decoding, this block modifies the strength of the watermarking, q, pixel by pixel.

In essence, the encoder determines whether the decoding will be accurate given the parameters A, B, and q. If the latter occurs, q is raised to the point where the bit can be appropriately decoded; otherwise, the controller moves on to evaluate the following bit embedding site. The data hidden in the host image (minutiae data or eigen-face coefficients) is recovered from the decoded watermark bits. The concealed face picture is recreated using the recovered eigen-face coefficients and the eigen-faces kept in the watermark decoding site. In the second application scenario, the original host fingerprint image's estimated location is also discovered by substituting the watermarked pixel values with the P (i,j) obtained by (2).

IX CONCLUSION

The capacity of biometrics-based personal identification methods to distinguish between a legitimate individual and a fraudster who unlawfully obtains an authorised individual's access privilege. One of the primary factors contributing to their appeal over conventional identification methods is the individual. The integrity and security of the biometric data themselves, however, are significant challenges. The methods of steganography, watermarking, and encryption for biometric data security are all viable options. Two uses of watermarking to safeguard that data are discussed in this study. Encryption is another method for enhancing the security of biometric data in addition to watermarking. The first use is enhancing the steganographic-based interchange of biometric data security. In the second application, inclusion of facial data into photographs of fingerprints. In this application, the data is concealed so that the fingerprint matching features are not considerably altered during encoding or decoding. As a result, the accuracy of verification based on decoded watermarked photos is extremely comparable to that of verification based on original photographs. To minimise the visibility of the host image modifications, the suggested technique makes use of numerous features of the human visual system. The capacity of the host pictures to hide data is currently being increased. Future studies could also look into the compatibility of various (such as robust and fragile) watermarking techniques.

REFERENCES

1. Ahmad A, Sinha GR, Kashyap N (2014) 3-level DWT image watermarking against frequency and geometrical attacks. Int J Comput Netw Inf Secur 6(12):58–63
2. Al-Afandy KA, El-Shafai W, El-Rabaie ESM, Abd El-Samie FE, Faragallah OS, El-Mhalaway A, Shehata AM, El-Banby GM, El-Halawany MM (2018) Robust hybrid water marking techniques for different color imaging systems. Multimed Tools Appl 77(19):25709–25759
3. Aslantas V (2009) An optimal robust digital image watermarking based on SVD using differential evolution algorithm. Opt Commun 282(5):769–777
4. Bajracharya S, Koju R (2017) An improved DWTSVD based robust digital image watermarking for color image. Int J Eng Manuf 1(11):49–59
5. Barni M, Bartolini F, Piva A (2001) Improved wavelet-based watermarking through pixel-wise masking. IEEE Trans Image Process 10(5):783–791
6. Chaitanya K, Reddy ES, Rao KG (2014) Digital color image watermarking in RGB planes using DWT-DCTSVD coefficients. Int J Comput Sci Inf Technol 5(2):2413–2417
7. Chen L, Zhao J (2018) Contourlet-based image and video watermarking robust to geometric attacks and compressions. Multimed Tools Appl 77(6):7187–7204
8. Divecha N, Jani NN (2013) Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images. In: Intelligent systems and signal processing (ISSP), 2013 international conference on. IEEE, pp 204–208
9. Gill R, Soni R (2017) An efficient image watermarking using 2-DCT and 2-DWT in color images. Int J Adv Res Comput Sci 8(5):1304–1308
10. Hsu LY, Hu HT (2017) Robust blind image watermarking using crisscross inter-block prediction in the DCT domain. J Vis Commun Image Represent 46:33–47
11. Jeswani J, Sarode T (2014) An improved blind color image watermarking using DCT in RGB color space. Int J Comput Appl 92(14):50–56
12. Kaur S, Jindal H (2017) Enhanced image watermarking technique using wavelets and interpolation. Int J Image Graph Signal Process 9(7):23– 35
13. Lin SD, Shie SC, Guo JY (2010) Improving the robustness of DCT-based image watermarking against JPEG compression. Comput Stand Inter 32(1–2):54–60
14. Nikolaidis N, Pitas I (1998) Robust image watermarking in the spatial domain. Signal Process 66(3):385–403
15. Parah SA, Sheikh JA, Loan NA, Bhat GM (2016) Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing. Digit Signal Process 53:11–24
16. Pradhan C, Rath S, Bisoi AK (2012) Non blind digital watermarking technique using DWT and cross chaos. Proc Technol 6:897–904
17. Raviya MKH, Kothari AM (2018) Comparative study of digital image watermarking based IJ Cox's algorithm versus proposed hybrid DWT-DCT approach. Eur J Acad Essays 5(5):98–104
18. Roy A, Maiti AK, Ghosh K (2018) An HVS inspired robust non-blind watermarking scheme in YCbCr color space. Int J Image Graph 18(03):1850015
19. Sheth RK, Nath VV (2016) Secured digital image watermarking with discrete cosine transform and discrete wavelet transform method. In: Advances in computing, communication, & automation (ICACCA)(spring), international conference on. IEEE, pp 1–5
20. Solachidis V, Pitas L (2001) Circularly symmetric watermark embedding in 2-D DFT domain. IEEE Trans Image Process 10(11):1741–1753
21. Su Q, Wang G, Jia S, Zhang X, Liu Q, Liu X (2015) Embedding color image watermark in color image based on two-level DCT. SIViP 9(5):991–1007
22. Tewari TK, Saxena V (2010) An improved and robust DCT based digital image watermarking scheme. Int J Comput Appl 3(1):28–32
23. Thanki R, Borra S (2018) A color image steganography in hybrid FRT-DWT domain. J Inf Sec Appl 40:92–102
24. Vaidya P, PVSSR CM (2017) A robust semi-blind watermarking for color images based on multiple decompositions. Multimed Tools Appl 76(24):25623– 25656

25. Wang Q, Ding Q, Zhang Z, Ding L (2008) Digital image encryption research based on DWT and chaos. In: Natural computation, 2008.ICNC'08. Fourth international conference on, vol 5. IEEE, pp 494–498
26. Xu H, Kang X, Wang Y, Wang Y (2018) Exploring robust and blind watermarking approach of colour images in DWT-DCT-SVD domain for copyright protection. Int J Electron Secur Digit Forensic 10(1):79– 96