Minor Project Report

Joint Encryption and Watermarking Scheme for Security of Medical Image

Under the guidance of:

Dr. Amit Kumar Singh

Assistant Professor

Submitted by:

Anant Malhotra (1806064)

Kalpesh Kumar Singh (1806059)

Smriti Pal (1806191)

Department of Computer Science and Engineering

National Institute of Technology Patna

May, 2021

Introduction

Due to advancement of Information and Communications Technologies (ICT), medical data is frequently and easily shared on the open network. Further, a lot of patient personal information and other significant medical data are stored on the server in primary healthcare centre and hospitals [2]. The ease of copying, manipulation, exchange, and distribution of images across the vulnerable public networks have brought forth the importance of providing security to exchanged medical images [1]. To provide safe transmission of medical images, there exists some security requirements that must be met. These requirements are confidentiality, authenticity, and integrity. Confidentiality states that only authorized users have access to the exchanged image, authenticity allows verification of the origin and owner of the exchanged image, and integrity ensures that the exchanged image has not been modified or tampered with.

Two technologies have been in common use to achieve the above security requirements: cryptography and digital watermarking. Cryptographic techniques scramble the medical image to achieve confidentiality, and use digital signatures to provide authenticity and integrity. However, with encryption only it is impossible to monitor how a legitimate user handles the content after decryption, thus making it possible to illegally redistribute or manipulate the content. The digital Watermarking technology seems to have the potential of fulfilling such a need as it embeds imperceptible information into the content, which is never removed during normal usage or causes inconvenience to the users. Digital watermarking authenticity and integrity are achieved by embedding control information as watermarks in the image, whereas confidentiality is not achieved [1]. Therefore, the implementation of a system that combines encryption standards with watermarking techniques and provides security to the medical images is the main concern of this article.

In this article, we develop a dual watermarking scheme in frequency domain to protect the EPR data for the healthcare system. The algorithm consists of two watermarks i.e., the text watermark (Patient's details) and the image watermark (Medical image). Each of these watermarks is first encrypted and then embedded in the cover image. The text watermark is encrypted using PN Sequence, while the image watermark is scrambled using Arnold Transform. Then, the first feature extraction of cover image is performed using DWT and the encrypted watermarks are embedded into the LH and HL sub bands. Finally, the watermarked image is encrypted using AES in CTR mode.

Literature Review

This section discusses related recent research works.

In the paper [2], a nonblind, dual watermarking technique is proposed that mainly comprises four major processes, i.e., watermark generation, insertion, CTE, and recovery of the generated watermark. This technique uses generated watermark where EPR data is first encoded using turbo code and then embedded into the wavelet coefficient of the watermark image. This generated EPR watermark is inserted into the redundant discrete wavelet transform (RDWT)-randomized singular value decomposition (RSVD) coefficient of the cover image. In the paper [4], visual cryptography-based grayscale image watermarking in DWT domain is proposed for copyright protection. The watermark image is split into two shares using (2,2) VC scheme. One of the shares is registered with the trusted authority and other is embedded in the low frequency domain of host image after feature extraction. Finally, the extraction process recovers original watermark by performing XOR operation between the shares. In the paper [5], an Elliptic Curve Cryptography centred encryption technique is used to encrypt the watermark and a DWT-SVD centred watermarking plan is used that explores 'U'

part acquired in the wake of captivating the SVD of low frequency band under various threshold standards. In the paper [3], five different cryptography algorithms are used to encrypt five different segments of the text message and the encrypted text message is hidden using LSB technique. The five different cryptography techniques used are Fibonacci series, PN sequence, XOR cipher, RSA and Hill cipher. In the paper [7], the methodology proposed is a new technique of dual image watermarking is proposed for protection of ownership rights which utilizes salient properties of homomorphic transform (HT), discrete wavelet transform (DWT), singular value decomposition (SVD) and Arnold transform (AT). In embedding algorithm host image is split into reflectance and illumination components using HT, DWT is further applied to the reflectance component resulting in frequency sub-bands (HL and LH) which are transformed by SVD. Two image watermarks are selected for embedding process whereas security of proposed algorithm is strengthened by performing scrambling of second watermark through AT. Both watermarks are transformed with DWT and SVD. Singular values (SVs) of both transformed watermarks are embedded into SVs of host image.

Preliminaries

A) PN Sequence

The Linear Feedback Shift Register (LFSR) has been one of the most popular encryption techniques widely used in textual communication. LFSR is suitable for text because text is continuous streaming data. They encrypt individual character (usually binary digits) of a plaintext message one at a time, using an encryption transformation which varies with time. Stream cipher which used LFSR is an algorithm that encrypts plaintext one bit at a time. Key stream or PN sequence generator generates outputs stream of bits k_1, k_2, ..., k_n. Cipher text is obtained by XORing this key stream bits with plain text bits p_1, p_2, ..., p_n.

$$c_i = p_i \oplus k_i$$

In synchronous stream ciphers, key stream is generated independent of the message being encrypted (decrypted). One key stream generator generates key stream of bits at the encryption side, another key stream generator generates the identical key stream of bits at the decryption end. For this method, the two key stream generators must be synchronized. If the key stream generators are not synchronized or one of cipher text bits is lost in transmission, then every cipher text bit is decrypted incorrectly. If this happens, sender and receiver must resynchronize the key generators. One advantage of synchronous stream ciphers is that they do not propagate transmission errors. If a bit is garbled during transmission only, that bit is decrypted incorrectly. If any active attacker inserts a bit into the cipher text stream and then it can be detected, the cipher text cannot be decrypted correctly after that inserted bit.

B) Arnold Transform

In practical applications, Arnold Transform not only scrambles the pixel position by only encoding the iterative number of the process, but also reduces the key spaces of storage and transmission. Thus, Arnold transform is introduced to implement image components scrambling. An image is attacked with the transformation which apparently randomizes the original organization of its pixels. Arnold period is the number of iterations, which depends on image size. Although there are many ways for scrambling, here Arnold transform [6] will be discussed, which is an iterative process to move the pixel position.

Suppose that an original image P is a N x N array, a pixel coordinate is
F = {(x, y) |x, y = 0, 1, 2, . . ., N – 1} [6], and then a two-dimension Arnold transform is expressed as

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_{n-1} \\ y_{n-1} \end{bmatrix} mod\ N$$

where x_n and y_n are transformed coordinates corresponding to xn1 and yn1 after n-iterations respectively, a and b are positive integers, and N is height or width of the square image processed. Since the transformation is an iterative process, if the location (x, y) is transformed several times, it returns to its original position after T-iterations. T is called as the period of transformation, and depends on parameters a, b and N. These parameters (a, b and N) can be used as secret keys. The pixels will continue to move until they return back to their original positions. Here, the moving time is T, and the size of pixel space is n = 0, 1, 2, . . ., N-1. Pixels move with periodicity. T, a, b and N (the size of original watermark) are correlated. Whenever the values change, a completely different Arnold cat map is generated [6]. After being multiplied a few times, the correlation among the pixels will be completely chaotic. To get back the original image, a periodicity is required. Suppose that the scrambling has performed n-iterations, then one can get the original image by per-forming T n-iterations.

C) Discrete Wavelet Transform

Wavelet theory was originally presented by J.Morlet, A.Grossman and Y.Meyer. Later Mallet and Daubechies provided the bonding between wavelet and signal processing. Wavelet transform overcome the limitation of Fourier transform of having both frequency and temporal information simultaneously. Discrete wavelet transform is based on sub band coding, which provides multiresolution analysis of digital signal. DWT can be achieved using digital filter banks. The signal is passed through different cut-off frequencies at various scales. If x[n] is original signal, it is passed through half band high pass filter g[n] and low pass filter h[n]. This results in 1-level decomposition, which is given by eqn 1 and eqn 2:

$$Y_{low}[k] = x[n] * h[2k-n] \qquad (1)$$

$$Y_{high}[k] = x[n] * g[2k-n] \qquad (2)$$

where $y_{low}[k]$ and $y_{high}[k]$ are the outputs of low and high pass filters respectively. The same process can be repeated to get the next level of decomposition. The reconstruction can be obtained using Inverse Discrete wavelet transform (IDWT), which is given by eqn 3:

$$x[n] = k\big(Y_{high}[k] * g[2k-n] + Y_{low}[k] * h[2k-n]\big) \qquad (3)$$

The DWT and IDWT of an image is obtained by applying wavelets separately to rows and columns of image. The DWT of an image results in 4 sub bands LL, HL, LH and HH as shown in fig. 1.

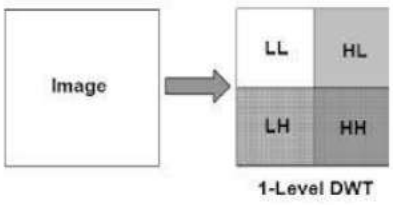


Fig.1 1- Level Discrete Wavelet Transform

D) AES

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128-bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14) [4, 6]. These rounds are governed by the following transformations:

(i) Bytesub transformation: Is a nonlinear byte substitution, using a substation table (s-box), which is constructed by multiplicative inverse and affine transformation.

(ii) Shiftrows transformation: Is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes.

(iii) Mixcolumns transformation: Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.

(iv) Addroundkey transformation: Is a simple XOR between the working state and the roundkey. This transformation is its own inverse.

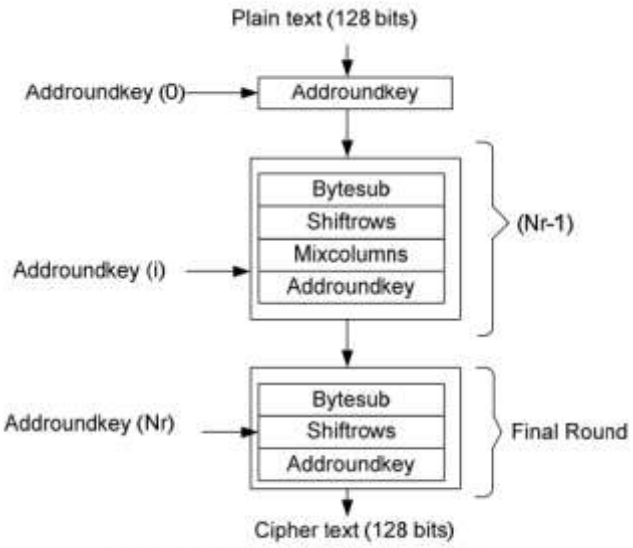


Fig.2 AES algorithm- Encryption Structure

The encryption procedure consists of several steps as shown by Fig. 2. After an initial addroundkey, a round function is applied to the data block (consisting of bytesub, shiftrows, mixcolumns and addroundkey transformation, respectively). It is performed iteratively (Nr times) depending on the key length. The decryption structure has exactly the same sequence of transformations as the one in the encryption structure. The transformations Inv-Bytesub, the Inv-Shiftrows, the Inv-Mixcolumns, and the Addroundkey allow the form of the key schedules to be identical for encryption and decryption.

In the case of **counter mode (CTR),** there is no need to implement a decryption algorithm of the block cipher. As shown in Figure 3, a 16-byte data block, called a counter, is encrypted by a block cipher in the place of plaintext. Then, this result and plaintext are merged by an XOR operation to create ciphertext. An n-bit counter is typically initialized to a pre-defined value (IV), and is then increased based on a pre-defined rule. The sequence of counter values must be distinguished from each other. In other words, the counter values must all have different values.

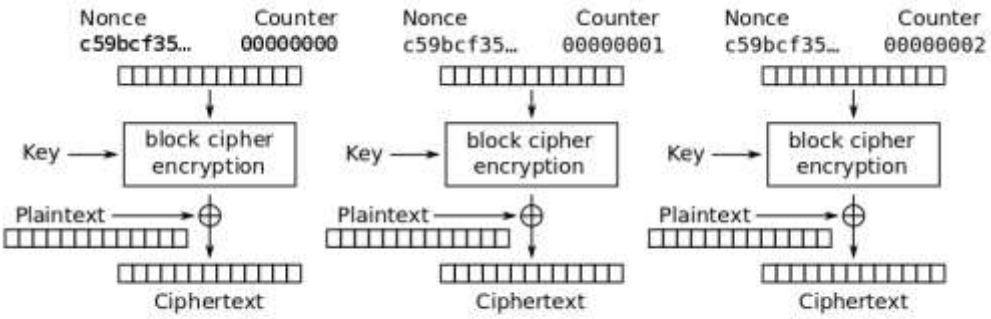
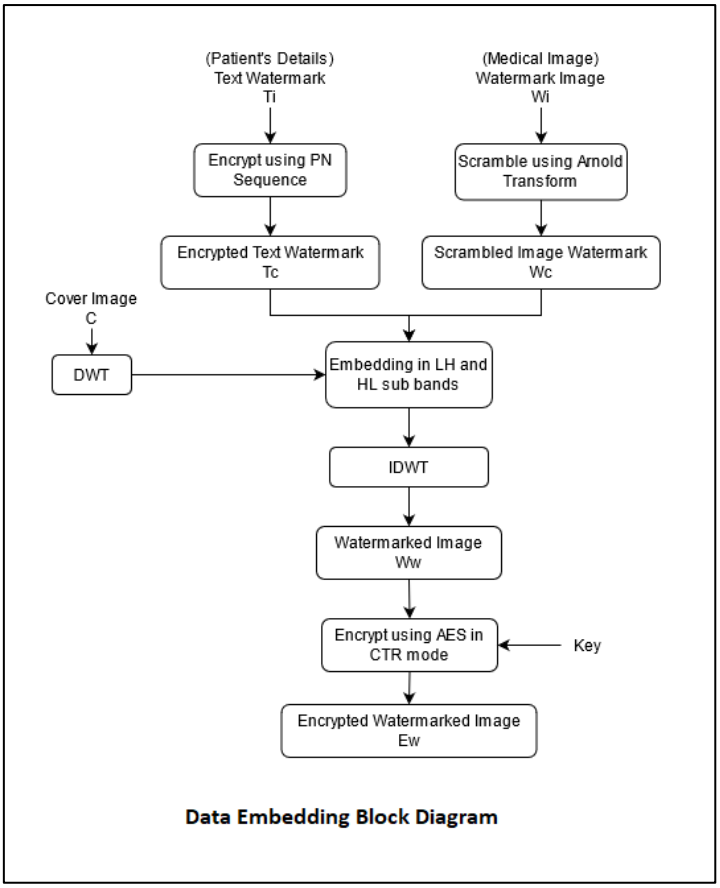


Figure 3. Counter (CTR) mode encryption

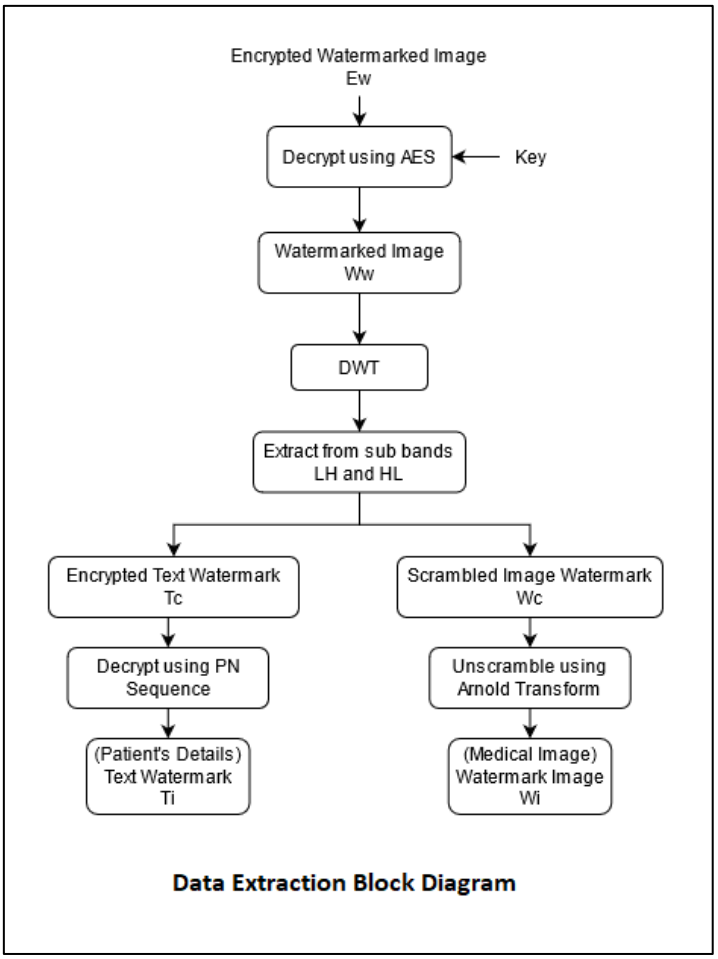
Proposed Method

In this article, a nonblind, dual watermarking technique is proposed that mainly comprises four major processes, i.e., watermark encryption and scrambling, imperceptible embedding, encryption of watermarked image using AES-CTR, and robust extraction of the watermarks.

In the watermark encryption and scrambling phase, the patient's details / Text Watermark (Ti) undergoes encryption via PN Sequence to produce Encrypted Text Watermark (Tc), and the Watermark Image (Wi) undergoes scrambling via Arnold Transform to produce Scrambled Image Watermark (Wc). In the next phase, these two watermarks are inserted into the LH and HL sub bands of the cover image (C) using DWT to obtain the watermarked image (Ww). Lastly, the watermarked image is encrypted using AES in CTR mode to produce the final Encrypted Watermarked Image (Ew). The below figures illustrate the entire model consisting of watermark encryption and scrambling, embedding, encryption of watermarked image, and extraction procedure.



Data Embedding Block Diagram



Data Extraction Block Diagram

Results and Analysis

In our proposed technique, a gray-scale image of size 512 x 512 is used as the host medical image, a gray-scale image of size 256 x 256 is used as the medical image watermark and a varying length string is used as the text watermark. Standard objective metric including Mean Squared Error (MSE), Peak-Signal-to-Noise Ratio (PSNR), Normalized Cross Correlation (NC), Bit Error Rate (BER), Structural Similarity Index (SSIM), Number of Changing Pixel Rate (NPCR), and Unified Averaged Changed Intensity (UACI) and subjective method are used to validate the performance of the proposed work. PSNR and SSIM are the measures of imperceptibility offered by any watermarking technique. Value of PSNR greater than 28 dB is acceptable. It can mathematically be described as

$$MSE = \frac{1}{X \times Y}\sum_{i=1}^{X}\sum_{j=1}^{Y}\left(I_{ij} - W_{ij}\right)^2 \qquad PSNR = 10\log\frac{(255)^2}{MSE}$$

Here, I_{ij} and W_{ij} are pixel of the original image of size X x Y and the watermarked image of size X x Y.

SSIM can be mathematically described as

$$p(a,b) = \frac{2\mu_a\mu_b + C_1}{\mu_a^2 + \mu_b^2 + C_1} \qquad q(a,b) = \frac{2\sigma_a\sigma_b + C_2}{\sigma_a^2 + \sigma_b^2 + C_2} \qquad r(a,b) = \frac{\sigma_{ab} + C_3}{\sigma_a\sigma_b + C_3}$$

where p(a,b), q(a,b), and r(a,b) are luminance comparison function, contrast comparison function, and structure comparison function, respectively.

Further, NC is used to determine the robustness offered by any watermarking technique. These can be described as

$$NC = \frac{\sum_{i=1}^{X}\sum_{j=1}^{Y}(W_{org_{ij}} \times W_{rec_{ij}})}{\sum_{i=1}^{X}\sum_{j=1}^{Y}(W_{org_{ij}}^2)} \qquad BER = \frac{(No.\ of\ incorrectly\ decoded\ bits)}{(Total\ number\ of\ bits)}$$

NPCR and UACI helps in describing the efficiency of the encryption scheme.

$$D(i,j) = f(x) = \begin{cases} 0, & C^1(i,j) = C^2(i,j) \\ 1, & C^1(i,j) \neq C^2(i,j) \end{cases}$$

$$NPCR = N(C^1, C^2) = \sum_{i,j}\frac{D(i,j)}{T} \qquad UACI = U(C^1, C^2) = \sum_{i,j}\frac{|C^1(i,j) - C^2(i,j)|}{F.T}$$

where C^1, C^2, F, and T are ciphertext images before and after pixel change, largest supported pixel value, and total number of pixels in ciphertext image, respectively.

The acceptable value = 36.7% (>33%) of UACI is obtained along with NPCR of 100% for AES – CTR Encryption on 512 x 512 Watermarked Image (Ww).

We evaluated our work by varying the gain factor (α) (At fixed character length = 22) and the results obtained are illustrated in Table 1. It is observed that the highest values of PSNR and SSIM obtained are 76.12 dB and 0.9999, respectively, at α = 0.001. However, the highest value of NC attained is 0.9962 at α = 0.5. Increasing the value of α improves the robustness, however, degrades the imperceptibility at the same time.

Table 1. Performance analysis at varying gain.				
Gain Factor (α)	**MSE**	**PSNR (dB)**	**SSIM**	**NC**
0.001	0.0015	76.12	0.9999	0.9960
0.005	0.0396	62.15	0.9995	0.9960
0.01	0.1586	56.13	0.9981	0.9961
0.05	3.9661	42.15	0.9565	0.9961
0.1	15.864	36.13	0.8553	0.9961
0.5	396.61	22.15	0.3450	0.9962

To further validate the suggested work, it is tested for text watermarks of different sizes (At fixed gain factor α = 0.005). The results for the same are produced in Table 2. We evaluated for length varying from 10 to 101 characters and got acceptable values of PSNR, NC and SSIM.

Table 2. Performance analysis for various length of text watermark.				
Text Size	**MSE**	**PSNR (dB)**	**SSIM**	**NC**
10	0.0396	62.15	0.9995	0.9960
22	0.0396	62.15	0.9995	0.9960
34	0.0396	62.14	0.9995	0.9960
50	0.0397	62.14	0.9995	0.9960
101	0.0398	62.13	0.9995	0.9960

Furthermore, the work is subjected to various attacks for testing the robustness and the values of standard metrics along with the visual displays are displayed in Table 3. The proposed work has achieved acceptable ranges of NC value (above 0.7) and BER (avg. value = 0.25) for all attacks except for rotation attack. for all attacks.

Table 3. Performance parameters for different attacks.			
Attack	**Noise Density**	**NC**	**BER (%)**
Salt & Pepper Noise	0.0001	0.9955	0
	0.001	0.9791	0
	0.01	0.8863	0
Gaussian Noise	Mean = 0, Var = 0.0005	0.9574	0
	Mean = 0, Var = 0.005	0.9406	0
	Mean = 0, Var = 0.05	0.9031	0.25
	Mean = 0, Var = 0.5	0.7353	0.50
	Mean = 1, Var = 0.0005	0.9559	0
	Mean = 1, Var = 0.005	0.9409	0
	Mean = 1, Var = 0.05	0.9008	0.25
	Mean = 1, Var = 0.5	0.7395	0.50
Speckle Noise	Mean = 0, Var = 0.0001	0.9361	0
	Mean = 0, Var = 0.001	0.8887	0
	Mean = 0, Var = 0.0025	0.8465	0.25
	Mean = 0, Var = 0.01	0.7626	0.25
	Mean = 0, Var = 0.025	0.7043	0.50
	Mean = 0, Var = 0.25	0.6337	1.00
JPEG Compression	QF = 10	0.8957	0.25
	QF = 50	0.9246	0
Rotation	1°	0.7361	2.25

Conclusion

The results show good performance in terms of imperceptibility, robustness, and security. Finally, the experimental analysis and good performance show that the proposed technique achieves an attractive tool for EPR data security for smart healthcare.

In future, we can implement machine learning, deep learning, and other optimization techniques to further improve the performance. We can also test the proposed work for some other practical applications.

References

[1]. H Abdel-Nabi and A Al-Haj, “Efficient Joint Encryption and Data Hiding Algorithm for Medical Images Security”, Proc. 8th Int. Conf. Inf. Commun. Syst. (ICICS), pp. 147–152, Apr. 2017.

[2]. A Anand A, A Singh, Z Lv, G Bhatnagar, “Compression-then-Encryption based Secure Watermarking Technique for Smart Healthcare System”, IEEE Multi-Media, pp 1–10, 2020.

[3]. A Kaur and S Singh, “A hybrid technique of cryptography and watermarking for data encryption and decryption”, IEEE, 2016.

[4]. P Kulkarni and G Kulkarni, "Visual Cryptography based Grayscale Image Watermarking in DWT domain", Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, pp. 1443-1446, 2018.

[5]. R Gupta, P Mundra, S Karwal, A Singh, “DWT-SVD based watermarking scheme of JPEG images using elliptic curve cryptography”, 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), pp. 359-365, 2016.

[6]. Y L Chen, H T Yau, G J Yang, “A maximum entropy-based chaotic time-variant fragile watermarking scheme for image tampering detection”, Entropy, Vol 15 pp 3170-3185, 2013.

[7]. P Khare and V K Srivastava, “A Novel Dual Image Watermarking Technique Using Homomorphic Transform and DWT”, J. Intell. Syst., vol. 30, no. 1, pp. 297–311, 2020.