A New Diffusion and Substitution-based Cryptosystem for Securing Medical Image Applications

L. Mancy and S. Maria Celestin Vigila
(Corresponding author: S. Maria Celestin Vigila)

Department of Information Technology, Noorul Islam University
Kumaracoil, Tamilnadu, India
(Email: mancy1989@gmail.com)

(Received Mar. 21, 2017; Revised and Accepted June 26, 2018; First Online July 11, 2019)

Abstract

In recent periods, individual security is becoming increasingly endangered. Several methods of safeguarding person are private, economic or health data are developed by entities, fabrications, and managements. Thus the patient data are generally produced in the place of the health images for observing. Thus, it is effortlessly available to each one. The patient data obviously shown may be interrupted by other parties during automated broadcast. For analysis purposes, these health informatics desires to be voluntarily nearby to the physicians. Unique feature of this scheme is to make a revision on the Digital Imaging and Communications in medicine (DICOM) standard, which specifies the form that all numerical health images will be well-suited. Several private data, such as patient's name, date of birth, gender, and patient identity with details about where the image was taken. So it is essential from the patient's idea of sight is to keep the above evidence in private. Therefore the security of medical images can be achieved through confidentiality, availability, reliability and authentication.

Keywords: Diffusion; Encryption; Histogram; Steganography; Substitution

1 Introduction

Cryptography has developed a communal, to afford an extraordinary defense against various attacks. It diminishes with the progression of systems for altering facts among reasonable and worthless practices. In endangered dispatches the cryptographic methods are focused by one or more keys. When the keys are same, are convoked as private key cryptography. Consecutively, when keys are different, then the cryptographic methods are known as public key cryptography. There are two vital assets which all encryption schemes must fulfill. The first is the confusion assets which involves, that cipher texts should have random advent. The second is the diffusion assets, which requires that alike keys should yield entirely contradictory cipher texts for the similar plaintext.

Digital imageries like hypnotic quality images, X-rays images, etc. are generally used in remedial solicitations. It compact with patient proceedings that are remote and should only obtainable to official folks. Though certain patients are unworried about rupture of privacy could root risky awkwardness and disgrace. Therefore, there is a necessity to defend and sustain privacy of patient information. In this dispatch, an endangered image encryption for DICOM images, based on the substitution and diffusion transformations is suggested. A secret key of 128-bits size is generated by an image a histogram. Initially, the visual feature of DICOM image is decomposed by the mixing process. The subsequent image is divided into key reliant blocks and further, these blocks are passed through diffusion and substitution processes. Total five rounds are used in the encryption method. Finally the generated secret key is embedded within the encrypted image in the process of steganography. At the receiver side the secret key was recovered from the embedded image and decryption operation was performed in inverse format. Here the Steganography is the art of secreting data by means that avoid the recognition of secret communications. It contains a huge amount of approaches to coat a communication from being grasped. The main aim of steganography is to distort the presence of any secreted statement.

The above introductory section explains the medical image security and provides some security measures to overcome the problem. The second section presents a review of literature and relevant research associated with the problem addressed in this study. Then the third section explains the methodology and the steps of the proposed cryptographic algorithm. Finally the fourth section explains the analysis of the data and the presentation of the results. Then the final section explains the conclusion

of medical image security applications.

2 Related Works

In the appraisal of works several researches have raised the safety of medicinal images in their own idea. Certain appropriate mechanism is highlighted in this section.

Zhou *et al.* introduced a technique certainty and reliability of digital mammography to encounter the necessities of authenticity and integrity of images [36]. Zhang *et al.* (2007) an image scrambling technique was established on queue transformation. Zhang *et al.* (2007) implemented a secured digital communication protocols under various conditions. Zhicheng *et al.* (2008) suggested a novel lossless data embedding technique. Michal Voss berg *et al.* (2008) acclimate the procedure to the globes grid safekeeping administration. Gouenou Coatrieux *et al.* (2009) familiarized to make the image more serviceable, by watermarking it with a precis data. Yong Feng *et al.* (2009) presented an invertible map, called Line map, for image crypto system.

Luiz Octavio Massato Kobayashi *et al.* (2009) a method using cryptography to improve conviction of medical images. Weihai Li *et al.* (2009) Peizhenwang *et al.* (2010) a better image encryption technique, which is based on hyper chaotic categorization is anticipated. Vinod Patidar *et al.* (2010) a diffusion-substitution system, based on chaotic map, for the image encryption is recommended. Sanfu Wangl *et al.* (2010) offered a image scrambling technique. Yi Wan *et al.* (2010) In this paper, a histogram based vigorous estimator for the noise mixing prospect was projected. Guiliang Zhul *et al.* (2010) recommended the three levels of multilayer scramble. Stallings (2010) has documented about security issues in his book. Sathish kumar *et al.*(2011) suggested anew algorithm for the image cryptographic system.

Thomas Neuberger *et al.* (2011) safeguards the medical accounts from prohibited access in which the patient as material container to resolve, who are the certified persons. Mustafa Ultras *et al.* (2011) authorize a secret scattering system, which segments the health images among a health team of 'n' doctors. Maria Celestin Vigila and Muneeswaran (2012) projected an Elliptic curvature based key generation for stream cipher. Dalel Bouslimi *et al.* (2012) advocate a mutual encryption watermarking method to combine the Quantization index modulation and an encryption algorithm. Abir Awad *et al.* (2012) a novel chaotic replacement method based on the complementary rule.

Musheer Ahmad and Tanvir Ahmed (2012) recommended a framework to provide visual protection to withstand statistical attacks to medical images. Li Chin Huangc *et al.* (2013) put forward a histogram fluctuating method to reach high bit depth health images. Tsang IngRen *et al.* (2013) estimated a motion recompense method to be applied in both encryption and decryption process. Maria Celestin Vigila and Muneeswaran (2013) the Elliptic curve cryptosystem for a text message was implemented. Chong Fu *et al.* (2013) offer a chaos medical image encryption pattern, through a bit-level shuffling process. Viswanathan *et al.* (2014) advocated by giving admission to the results of medical images with secrecy, convenience and veracity. Abhilasha Sharma *et al.* (2015) direct the watermarking method based on DWT to embed multiple watermark into the cover image. Jani Anbarasi *et al.* (2015) anticipated a multi top-secret image sharing scheme that shares the multiple disruption polynomial.

Mancy and Maria Celestin Vigila (2015) reviewed on image encryption technique and their functionalities are analyzed. Maria Celestin Vigila and Muneeswaran (2015) proposed the implementation of reversible information hiding in spatial domain images rooted in neighbor mean image interruption without impairing the image eminence. ZeinabFawaz *et al.* (2016) a novel image encryption scheme based on two rounds of substitution–diffusion is proposed. Ritu Agrawal *et al.* (2016) uses a lossless medical image watermarking method using modulation variation was implemented, which offers high healthiness and low entropy distance for safeguard. Akram Belazi *et al.* (2016) a novel image encryption approach based on permutation substitution network and chaotic systems are proposed. BalaKrishnan Ramalingam *et al.* (2017) present permutation and diffusion based hybrid image crypto system in transform domain using combined chaotic maps and Haar Integer Wavelet Transform. Weijia Cao *et al.* (2017) presents a medical image encryption algorithm using edge maps derived from a source image. Shahryar Toughi *et al.* (2017) utilize the Elliptic curve generator to generate a sequence of arbitrary numbers based on curves.

3 The Proposed Methodology

The medical image safety has become a significant problem during the storage and broadcast of data. So to preserve the conveyed proof beside undesirable description, the secret key used in encryption process is generated from the image itself. By mixing process, the distinctive pixel is extended by associating the present pixel with its former pixel and its session key. Here the size of the block is decided by session key, in which the block may be of any one of the ten different sizes. Then in diffusion process, the pixel of each block is reorganized within the block by a spiral path pattern. In the substitution process, the pixel of each block is changed with one of their nearby pixels. Finally the generated secret key is embedded into the cipher image using the process of steganography.

To secure the medical DICOM image, the secret key of 128 bit size is generated by an image histogram. Then the medicinal image is encoded by using diffusion and substitution procedure. Total five rounds are used in the encryption method. At last the secret key is fixed within the encrypted image by the method of steganography. At the receiver side the key was recovered from the embedded

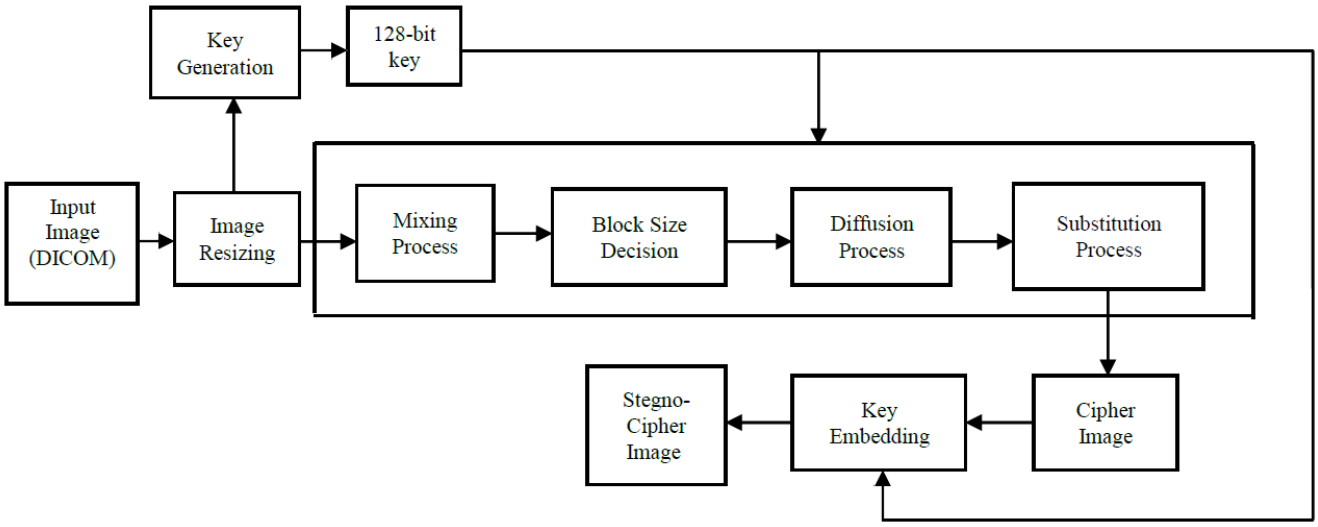

Figure 1: Block diagram of the proposed methodology

image and then decryption operation is performed in the inverse setup. Fig 1 shows the block diagram of proposed approach.

The steps of this proposed cryptographic algorithm is explained as follows.

1) Key generation:
The private key assets in the encryption process are generated from the image itself.

Step 1. At first the histogram of the image is calculated by means of histogram counts.

Step 2. Then histogram counts of 255 values are obtained by dividing the i^{th} count by $i+1^{th}$ count.

Step 3. The obtained result is rounded to the nearest integer and modulo10 operation is performed on the values.

Step 4. The resulting values will be in the range of [0-9].

Step 5. From the 255 values, the first 128 values are extracted and formed as a secret key with a size of 128 bits.

Step 6. Then this key is divided into block of 8 bits to form the session keys $k = k_1 k_2 \cdots k_{32}$ (in hexadecimal) given as $K = K_1 K_2 \cdots K_{16}$ (in ASCII).

Here, k_i's referred to as sub-keys are hexadecimal digits (0-9 and A-F) and K_i represents the session keys.

2) Mixing Process:
In mixing process every pixel of the image is interchanged with its earlier pixels and the session key by XOR operation. The algorithm related to mixing process is given in Algorithm 1. In this algorithm, 'H' and 'W' represent the Highness and Extensiveness of the image respectively; $P_{x,0} = \{0$ when $x = 1$ & $P_{x-1,W}$ when $x > 1\}$.

Algorithm 1 The mixing process

```
i ⟵ position of first session key, i.e. 1
for x = 1: H do do
  for y = 1: W do do
    P_{x,y} ⟵ (P_{x,y} ⊕ P_{x,y−1} ⊕ K_i)
    i ⟵ position of next session key, i.e. ((i mod 16) + 1)
  end for
end for
```

3) Block Size Decision:
The resulting image from the mixing process is divided into non-coinciding blocks B 1, B2....BN. Here the size of the block is decided by session key Ki .The block may be of any one of the ten different sizes. So, total five rounds are used to complete the encryption process. In each round unique session key Ki is used. The table1 shows the block size decision criteria.

4) Diffusion Process:
Here the scrambling of the image is based on spiral scanning pattern. Here the scrambling is done in a key dependent manner. The Pixel of each block is replaced within the same block by a spiral path of size 8×8 matrix. Location of the starting pixel for navigating in a block is made key reliant on exclusively. For this purpose pairs of neighboring sub keys are formed. The Key pairs are given as (k_1, k_2), (k_3, k_4),(k_5, k_6), (k_7, k_8) and (k_1, k_2). When all sub-key pairs are firmed it is commenced again from the first sub-key pair (k_1, k_2). At the end of diffusion processes, not only all pixels get altered, but also their neighboring pixels are rearranged broadly within the

Table 1: Block size decision table

K_i mod 10	0	1	2	3	4	5	6	7	8	9
Block Size (B_i)	16	24	32	40	48	56	64	72	80	96

image block. The 8×8 matrix diagram is given in Figure 2.

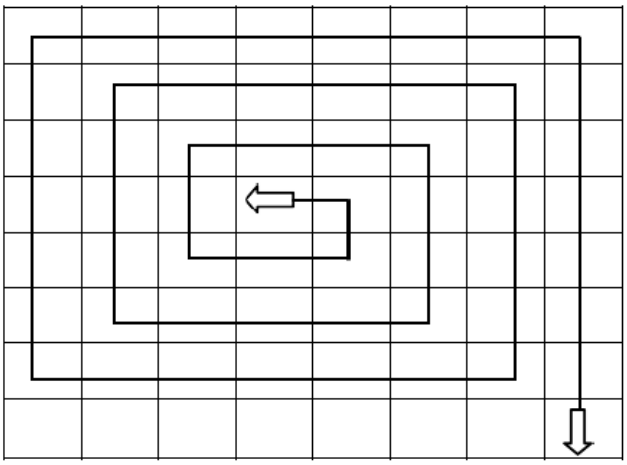

Figure 2: Spiral path Scrambling

5) Substitution Process:
In substitution process the property of the selected pixel is altered by the one of the neighboring pixels in the eight directions (i.e.) the current pixel is XOR-ed with the neighboring pixel. Therefore the eight neighboring pixels are North, North West, North East, South, South West, South East, East (E) and West (W). Here, we use neighboring as $P_{x,y}$ which is XOR-ed with current pixel $P_{i,j}$. When all the sub-keys are shattered, begin the procedure from the first sub-key k_1 again. In this step, some of the pixels lying on the boundary of a block may be remain unaffected. The pixel location table is given in Table 2.

6) Key Embedding:
The generated secret key is embedded into the cipher image using DWT transform, which is applied to the image to form four sub bands such as LL, LH, HL and HH. The LL level is obtained to the size of 128×128. Then the transformed coefficients in all the bands are converted into the binary form and along the diagonal elements the 3 LSB is replaced with each bit of the secret key after converting each digit in binary form with three digits. Then after implanting the secret key is transformed into decimal format and again, it is converted into original format by IDWT. The ultimate output is the embedded image and the secret key is mended at the receiver side through extraction process and the image is decrypted in the reverse order as done in the encryption stage.

Table 2: Pixel location table

Sub Key value k_i	Directions of adjacent surrounding pixel to a pixel	Location Surrounding pixel $P_{x,y}$ w.r.t current pixel
0/F	E	$P(i, j+1)$
1/E	NE	$P(i-1, j+1)$
2/D	N	$P(i-1, j)$
3/C	NW	$P(i-1, j-1)$
4/B	W	$P(i+1, j-1)$
5/A	SW	$P(i+1, j)$
6/9	S	$P(i+1, j)$
7/8	SE	$P(i+1, j+1)$

4 Performance Analysis

The current scheming power is capable of breaking encryption patterns in a real time, if the scheme is not designed to look into these problems. Hence, a good encryption system would preserve away from the possible attacks. Hence, analysis of encryption systems such as histogram analysis, Entropy, Correlation analysis, etc., certifies the precise growth of the security scheme.

1) Statistical Analysis:
The statistical analysis involves collecting every data sample in a set of items from which samples can be drawn. The different types of statistical analysis are given as follows.

   a. Histogram Analysis:
   A histogram is a graphical design of numerical data. An image histogram is a chart that shows the dispersal of intensities in a grayscale image. To prevent the outflow of data to an opponent, it is substantial to guarantee that the cipher image does not have any statistical resemblance to the input image. The histogram of the input image has massive sting. But, the histogram of the cipher image is nearly even and constant, signifying the nearly same probability of existence of each intensity level. Figure 3 shows the histogram of original, cipher and stegno image.

   b. Information Entropy:

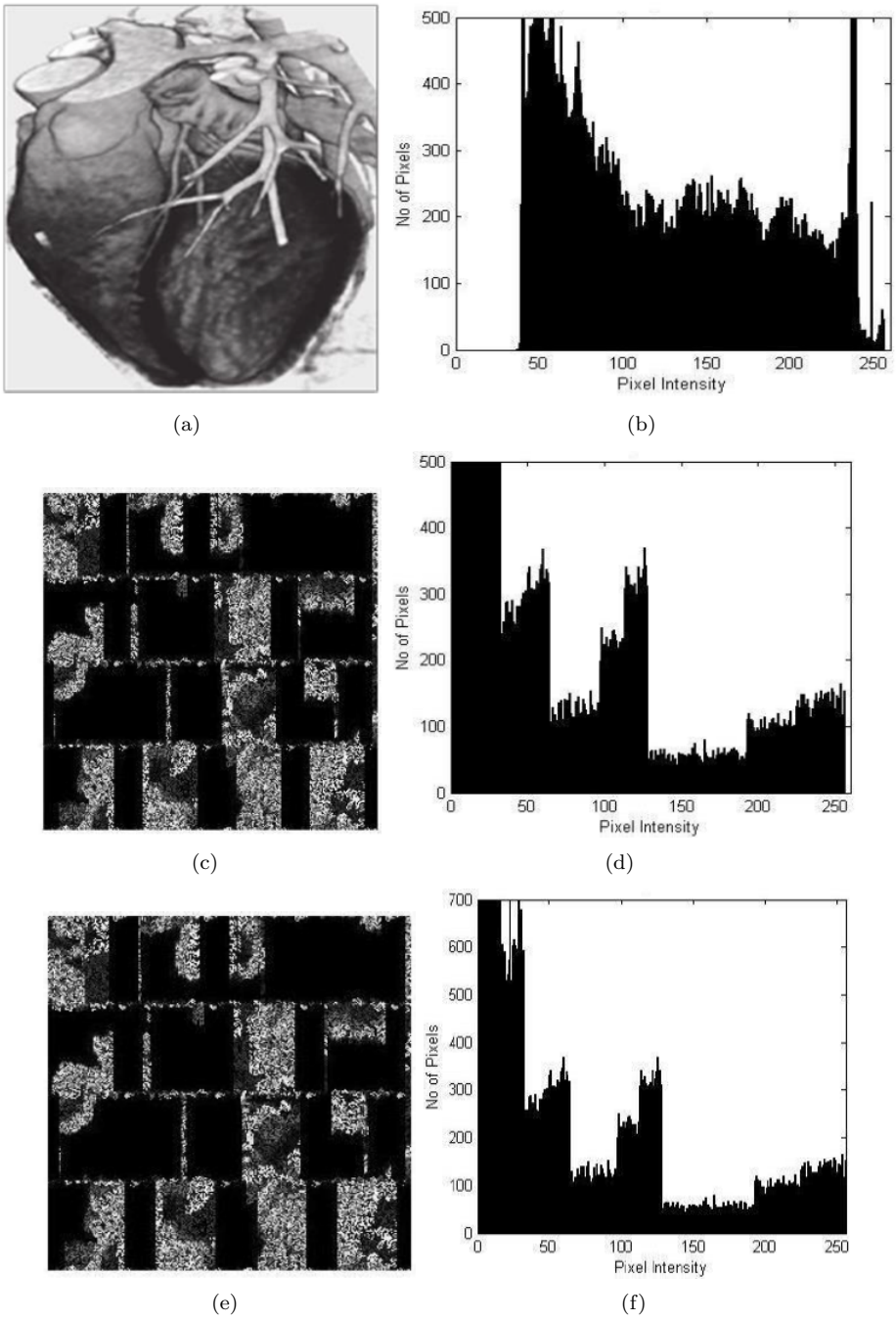

Figure 3: Histogram of original, encrypted, and stegno-cipher Images. (a)Original Image, (b) Histogram of Original Image, (c) Encrypted Image , (d) Histogram of Encrypted Image, (e) Stegno-Image, (f) Histogram of Stegno Image.

Information entropy is a concept from information theory. It tells how much information there is at an event. In general, the more uncertain or random the event is, the more information it will contain. It has applications in many areas, including lossless data compression, statistical inference, cryptography, etc. The Entropy calculation formula gives as follows,

$$H(s) = \sum P(S_i) \log 2 \times (1/P(S_i)). \quad (1)$$

Where $P(S_i)$ is the probability of an i th image. Table 3 shows the entropy of original, cipher and stegno image. To enterprise a good image encryption pattern, the entropy of encrypted image should be closer to the ultimate expected value 8. Therefore the information outflow in the proposed cipher is insignificant, and it is safe upon the entropy outbreak.

2) Correlation Analysis:
The correlation is an arithmetic method that shows

Table 3: Entropy of original, cipher and plain image

Image	Entropy
Original Image	7.2551
Cipher Image	7.5564
Stegno Image	7.6463

whether and how powerfully the couples of variables are connected. The correlation between pairs of original and its corresponding encrypted image produced using the proposed image encryption algorithm by computing the correlation coefficients. The formula related to correlation coefficients are given as follows.

$$\begin{aligned} C_{x,y} &= cov(x,y)/\sqrt{D(x)}\sqrt{D(y)} \\ E(x) &= 1/N \times \sum x_i \\ D(x) &= 1/N \times \sum (x_i - E(x))^2 \\ Cov(x,y) &= 1/N \times \sum (x_i - E(x))(y_i - E(y)). \end{aligned}$$

In the given formula, there are N pairs of neighboring pixels and x, y represent the intensity values of two neighboring pixels from an image. Table 4 shows the correlation of original, cipher and stegno images.

3) Key Sensitivity Analysis:
Even a variation in a single bit of the key will make an entirely different cipher image for the attackers to identify the key. This makes the encryption procedure sensitive enough to the secret key. To test the sensitivity of the proposed image cipher with respect to the key, encrypted image corresponding to plain image is decrypted with a slightly different key than the original one. Here the two cipher images are associated, in which it was not easy to compare the cipher images by simply observing these images. Thus, for comparison, the correlation between the identical pixels of the two cipher images is intended. Table 5 shows the entropy and correlation between two cipher images.

Here Figure 4 shows the Key Sensitivity Analysis of original and two cipher images. Therefore a perfect diffusion and substitution method should resist against all kinds of attacks. Hence some analysis techniques such as statistical, correlation and key sensitivity analysis are discussed in the above session to prove that the proposed algorithm is secretive against most common attacks. Therefore a new diffusion and substitution based cryptosystem for securing the medical image applications is implemented and performance analysis designates that the proposed cipher is more secure.

5 Conclusion

To secure the medical image, the secret key of 128 bit size is generated by means of image histogram and the medical image is encrypted by using diffusion and substitution process. Finally the secret key is embedded within the encrypted image in the process of steganography. This also enriched the security of medical image. At the receiver side the key was recovered from the embedded image and then decryption is performed in the reverse format. Due to this, the security of medical image is enriched. Here we deliberate the security analysis of medical image encryption pattern such as statistical analysis, correlation analysis and key sensitivity analysis, which prove that the proposed cipher is safe against the most common attacks.

References

[1] R. Agrawala, M. Sharma, "Medical image watermarking technique in the application of diagnosis using M-ary modulation," in *International Conference on Computational Modeling and Security*, 2016.

[2] M. Ahmed, T. Ahmed, "A framework to protect patient digital imagery for secure telediognosis," *Procedia Engineering*, vol. 38 , pp. 1055-–1066, 2012.

[3] J. S. Anbarasi, A. G. S. Malab, M. Narendrac, " DNA based multi-secret image sharing," in *International Conference on Information and Communication Technologies*, 2015.

[4] A. Awad and A. Miri, "A new image encryption algorithm based on a chaotic dna substitution method," in *IEEE International Conference on Communications (ICC'12)* , 2012.

[5] A. Belazi, A. A. Abd El-Latif, S. Belghith, "A novel Image Encryption Scheme based on Substitution-Permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[6] D. Bouslimi, G. Coatrieux, M. Cozic, C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, pp. 5, pp. 891–899, 2012.

[7] W. Cao, Y. Zhou, C. L. P. Chen, L. Xia, "Medical image encryption using edge maps," *Signal Processing*, vol. 132, pp. 96–109, 2017.

[8] G. Coatrieux, C. Le Guillou, J. M. Cauvin, "Reversible watermarking for knowledge digest embedding and reliability control in medical images," *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 2, pp. 158—165, 2009.

[9] Z. Fawaz, H. Noura and A. Mostefaoui, "An efficient and secure cipher scheme for images confidentiality preservation," *Signal Processing*, vol. 42, pp. 90–108, 2016.

[10] Y. Feng, X. Yu, "A novel symmetric image encryption approach based on an invertible two-dimensional map," in *35th Annual Conference of IEEE Industrial Electronics*, pp. 4244–4649, 2009.

Table 4: Correlation of original, cipher and stegno images

Image	Vertical Correlation	Horizontal Correlation	Diagonal Correlation
Original Image	-0.0053	-0.0075	-0.0068
Cipher Image	-0.0063	-0.0042	-0.0130
Stegno Image	-0.0089	-0.0032	-0.0073

(a) (b) (c)

Figure 4: Key sensitivity analysis of original, cipher image 1 and cipher image 2. (a)Original Image, (b) Cipher Image 1, (c) Cipher Image 2.

Table 5: Entropy and Correlation between two cipher images

Image	Entropy	Vertical Correlation	Horizontal Correlation	Diagonal Correlation
Cipher Image 1	7.5564	-0.0063	-0.0042	-0.0130
Cipher Image 2	7.6463	-0.0089	-0.0032	-0.0073

[11] C. Fu, W. H. Meng, Y. F. Zhan, *et al.*, "An efficient and secure medical image protection scheme based on chaotic maps," *Computers in Biology and Medicine*, vol. 43, pp. 1000–1010, 2013.

[12] L. C. Huang, L. Y. Tseng, M. S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images," *The Journals of Systems and Software*, vol. 86, pp. 716–727, 2013.

[13] L. O. M. Kobayashi, S. S. Furuie, P. S. L. M. Barreto, "Providing integrity and authenticity in DICOM images: A novel approach," *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 4, pp. 582–589, 2009.

[14] W. Li, Y. Yuan, " Improving security of an image encryption algorithm based on chaotic circular shift," in *IEEE International Conference on Systems and Cybernetics*, 2009.

[15] L. Mancy, S. M. C. Vigila, "A survey on protection of medical images," in *International Conference on Instumentation, Communication and Computational Technologies*, 2015.

[16] T. Neubauera, J. Heurixb, "A methodology for the pseudonymization of medical data," *International Journal of Medical Informatics*, vol. 80, pp. 190–204, 2011.

[17] Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun, X. Lin, "Robust lossless image data hiding designed for semi fragile image authentication," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 18, no. 4, pp. 497—509, 2008.

[18] V. Patidar, G. Purohit, K. K. Sud, N. K. Pareek, "Image encryption through a novel permutation-substitution scheme based on chaotic standard map," in *International Workshop on Chaos-Fractal Theory and Its Applications*, 2010.

[19] B. Ramalingam, A. Rngarajan, J. B. B. Rayappan, " Hybrid image crypto system for secure image communication - A VLSI approach," *Microprocessor and Micro Systems*, vol. 50, pp. 1–13, 2017.

[20] C. C. Sabino, L. S. Andrade, T. I. Ren, G. D. C. Cavalcanti, T. I. Jyh, J. Sijbers, "Motion compensation techniques in permutation-based video encryption," in *IEEE International Conference on Systems and Cybernetics*, 2013.

[21] G. A. Sathishkumar, K. B. Bagan, N. Sriraam, "Image encryption based on diffusion and multiple chaotic maps," *International Journal of Network Security & Its Applications*, vol. 3, pp. 2, pp. 181—194, 2011.

[22] A. Sharma, A. K. Singh, S. P. Ghrera, "Secure hybrid robust watermarking technique for medical images," in *International Conference on Eco-friendly Computing and Communication Systems*, 2015.

[23] W. Stallings, *Cryptography and Network Security*, Fifth Edition, 2010.

[24] S. Toughi, M. H. Fathi, Y. A. Sekhavat, " An image encryption scheme based on elliptic curve pseudo random and advanced encryption system," *Signal Processing*, vol. 141, pp. 217–227, 2017.

[25] M. Ulutas, G. Ulutas, V. Nabiyev, "Medical image security and EPR hiding using Shamir's secret sharing scheme," *The Journals of Systems and Software*, vol. 84, pp. 341–353, 2011.

[26] S. M. C. Vigila, K. Muneeswaran, "Key generation based on elliptic curve over finite prime field," *International Journal on Electronic Security and Digital Forensics*, vol. 4, pp. 1, pp.65—81, 2012.

[27] S. M. C. Vigila, K. Muneeswaran, "A new elliptic curve cryptosystem for securing sensitive data applications," *International Journal on Electronic Security and Digital Forensics*, vol. 5, pp. 1, 2013.

[28] S. M. C. Vigila, K. Muneeswaran, "Hiding of confidential data in spatial domain images using image interpolation," *International Journal of Network Security*, vol. 17, No. 6, pp. 722–727, 2015.

[29] P. Viswanathan, V. P. Krishna, "A joint FED watermarking system using spatial fusion for verifying the security issues of teleradiology," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 3, 2014.

[30] M. Vossberg, T. Tolxdorff, "DICOM Image Communication in Globus-Based Medical Grids," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, pp. 2, pp. 145—153, 2008.

[31] Y. Wan, Q. Chen, Y. Yang, "Robust impulse noise variance estimation based on image histogram," *IEEE Signal Processing Letters*, vol. 17, no. 5, pp. 485—488, 2010.

[32] P. Wang, H. Gao, M. Cheng, X. Ma, "A new image encryption algorithm based on hyperchaotic mapping," in *International Conference on Computer Application and System Modeling*, 2010.

[33] S. Wang, Y. Zheng, Z. Gao, " A new image scrambling method through folding transform," in *International Conference on Computer Application and System Modeling*, 2010.

[34] H. Y. Zhang, "A new image scrambling algorithm based on queue transformation," in *International Conference on Machine Learning and Cybernetics*, pp. 19–22, 2007.

[35] J. Zhang, F. Yu, J. Sun, Y. Yang, C. Liang, "DICOM image secure communications with internet protocols IPv6 and IPv4 ," *IEEE Transactions on Information Technology in Bio medicine*, vol. 11, no. 1, pp. 70—80, 2007.

[36] X. Q. Zhou, H. K. Huang, and S. L. Lou, "Authenticity and integrity of digital mammography images," *IEEE Transaction on Medical Imaging*, vol. 20, pp. 8, pp. 784—791, 2001.

[37] G. Zhu, W. Wang, X. Zhang, M. Wang, " ZGW-1 digital image encryption algorithm based on three levels and multilayer scramble," in *2nd IEEE International Conference on Network Infrastructure and Digital Content*, 2010.

Biography

S. Maria Celestin Vigila completed her B.E. in Computer Science and Engineering in 1996 and M.E. in Computer Science and Engineering in 1999. She completed her Ph.D. in the area of data security from Anna University, Chennai. She is currently Associate Professor in the Department of Information Technology, Noorul Islam University, Kumaracoil and member of ISTE and IET. She is the reviewer for quite a few peer reviewed international journals. Her research interest includes cryptography and network security, wireless networks and information hiding.