A Joint SVD based Watermarking and Encryption Scheme using Chaotic Logistic Map

Monjul Saikia[1] and **Swanirbhar Majumder**[2], Non-members

ABSTRACT

Copyright protection and secrecy of some sensitive data is essential in this present digital era which deals with the advances in cloud computing and big data analytics. Digital watermarking is a popular method for copyright protection whereas cryptography takes care in hiding information as well as for secure transmission of data in a manner that is unreadable to a third party. Combination of both these techniques enhances the security and copyright protection aspects for the concealment of transmitted information. This paper presents a way of achieving those by combining both of these methods together as a joint scheme. Here a robust SVD based algorithm is proposed for embedding a watermark on a host image and then encrypts the resultant stego-image using chaotic logistic map in DCT coefficients. The decryption process is non-blind and requires the help of the key used in encryption. The joint algorithm has been found to be image independent due to its good performance for several popular test images.

Keywords: Chaos; Logistic map; Partial Encryption; Block Cipher, DCT, SVD.

1. INTRODUCTION

These days with the wide and varied availability of multimedia data, Image encryption and copy right protection is dealt with in abundance. They have found a lot of focus in the field of signal processing. There are various multimedia signals like text, audio, image and video. Some of these are multi dimensional or multi channel signals and some combination of both. Here of these different multimedia signals the algorithm discussed is for security and copyright protection, and has been applied on color images. The color images are multi channel and multi dimensional signals i.e. the 3 channels for the R(red), G (green) and B (Blue) as well as 2 dimensions (row and columns of the individual channels).

Manuscript received on August 31, 2014 ; revised on May 6, 2015.

Final manuscript received on July 25, 2015.

[1] The author is with Department of Computer Science and Engineering, NERIST, Nirjuli, Arunachal Pradesh, India, E-mail: monjuls@gmail.com

[2] The author is with Department of Electronics and Communication Engineering, NERIST, Nirjuli, Arunachal Pradesh, India, E-mail: swanirbhar@ieee.org

In most of the images, the value of the pixels can be predicted from its nearby pixel values. For any image encryption/decryption operation, encoding is the process in which original images represented in some other form to protect it against eavesdroppers, while decoding is the process to obtain or recover the original image from the encoded image. Among two processes for secure image encryption namely full encryption and partial encryption, the full encryption algorithm encrypts complete data, which can obtain high security. But they are of high computation complexity and change the file format. Whereas, partial encryption algorithm obtain high speed by encrypting only some sensitive data so it is more suitable for most application.

As chaos based maps are considered similar to ideal ciphers as they have the properties of sensitivity to initial condition or system parameters like confusion, diffusion, balanced and avalanched property etc. Therefore a number of chaotic image encryption schemes have been proposed recently. In this paper, the idea of encryption scheme using chaotic logistic map given by Pareek et. al. [1] has been combined with our previously published watermarking algorithm. Moreover the novel idea of combining encryption with watermarking has been incorporated. Therefore to meet the requirement of the secure image transfer, a new partial image encryption scheme is proposed DCT (discrete cosine transform) based on chaotic logistic map diffusion. To enhance it, before encryption a secure SVD (singular value decomposition) based watermarking technique has been employed to watermark the host image with a logo.

An image logo has been hidden in the host image, followed by the encryption of the image. In this image an 80-bit external secret key has been used for image encryption scheme and two chaotic logistic maps have been applied. The initial conditions for both logistic maps are derived using the secret key by providing different weightage to its bits. For watermarking the SVD based watermarking scheme of our previously published papers has been used. For encryption in the algorithm, the first logistic map is used to generate numbers ranging from 1 to 24. The initial condition of the second logistic map is modified from the number generated by the first logistic map. By modifying the initial condition of the second logistic in this way, its dynamics get further random-

ized. In the proposed algorithm, DCT is performed on the given image. Over these DCT values nine different types of operations were performed to encrypt the selective pixels of the watermarked image. The operation to be performed over the particular pixel is decided by the outcome of the second logistic map. Thus the second chaotic map further increases the confusion in the relationship between the encrypted and its original image. To make the cipher more robust against any attack, after each encryption of 15 pixels from a block, the secret key is modified to make it untraceable for malicious attackers.

2. PREVIOUS WORK

The chaotic logistic map based image encryption technique proposed by N.K.Pareek, Vinod Ptidar and K.K.Sud[1] presents an algorithm which utilizes two chaotic logistic maps and an external key of 80 bits. To encrypt the pixels of an image eight different types of operations are used. Another chaotic logistic map technique have been proposed by Mrinal Kanti Mandal, Gourab Dutta Banik, Debasish Chattopadhyay and Debashis Nandi [2]. This technique was employed on the gray level where the XOR operations and pixel shuffling of the image are used to confused and diffuse the pixel value and the pixel position.

In the above techniques, the entire image is encrypted and decrypted each time, which is a big overhead in case of storage and retrieval of large set of images, in an image database or transmission of images over large an insecure channel. Also the loss of even a small part of the encrypted images results in greater distortion in the decrypted image. This is due to the fact that the part of the encrypted image which is distorted constitutes pixels that will be scattered in the decrypted image. The watermark embedding and decoding schemes employed involves the basic system algorithm of Majumder et.al as in [12-17].

3. SELECTIVE IMAGE ENCRYPTION

It is well known that images are different from texts in many aspects, such as high redundancy and correlation. For the properties of large volumes and large computational time, the traditional ciphers like Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES), RSA algorithm (Rivest-Shamir-Adleman) etc are not suitable for real time image encryption. An encryption method, which takes large computational time but may have very good security feature would be of little practical use for real time processes.

IDEA most of which are used in text or binary data. So it is difficult to implement it directly on multimedia data. As multimedia data are of high redundancy, of large volumes and require real-time interactions. So directly applying these ciphers displaying, cutting, copying, bit rate conversion etc. with videos are time consuming and not suitable for real time. The block diagram for partial encryption and decryption is as in figures 1 and 2. Though in this paper simulations have not been implemented on hardware to substantiate real time implementation, but in future these may be used for the same. Therefore , for the sake of real time simulation, the encryption as well as watermarking algorithms have to be implemented in hardware platform.

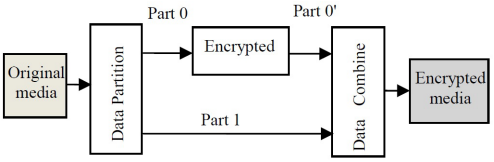

Fig.1: *Partial Encryption.*

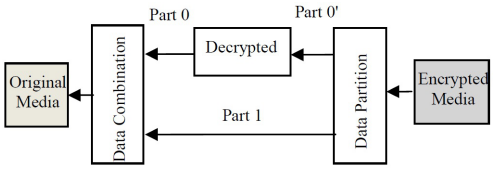

Fig.2: *Partial Decryption.*

4. CHAOTIC LOGISTIC MAP

From the word 'chaos' we understand that "the sensitivity to initial condition". Chaos theory shows the difficulty of predicting their long-range behavior [1]. Recently, one simple chaotic map has been studied for cryptography application is logistic map. Mathematically, the logistic map is written as:

$$f(x_n) = rx_n(1 - x_n)$$
$$x_{n+1} = f(x_n)$$

where, x_n represents the chaotic sequence[2] which lies between zero and one as shown in figure 3. The initial condition of the map is $x_{n=0} = x_0 \in [0, 1]$. The parameter r is a positive real number in the range 0 and 4. The researcher shows that the system is in chaotic state under the condition that $3.56994 < r \leq 4$ [1]. But r beyond 4, the value of x_n eventually leaves the interval [0,1] and x_n diverge for almost all initial values of x_0. Chaotic behavior and variation of r, x are shown in figure 3 and figure 4 respectively. Also it is seen that maximum variation of x_n is found to be for choosing constant r in the range of $3.56994 < r \leq 4$.

High flexibility in choosing an initial condition of chaotic logistic map, unpredictability of $f(x_n)$ after n iteration and also efficiency in computation of chaotic signal makes it suitable for the encryption of large bulky data.

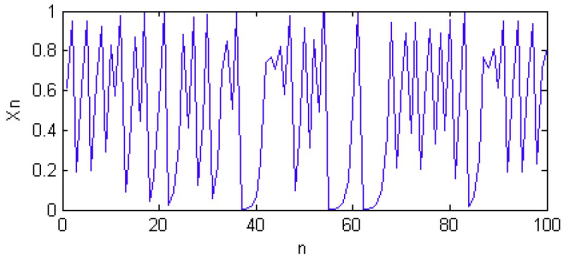

Fig.3: *Variation of chaotic logistic map with iteration values.*

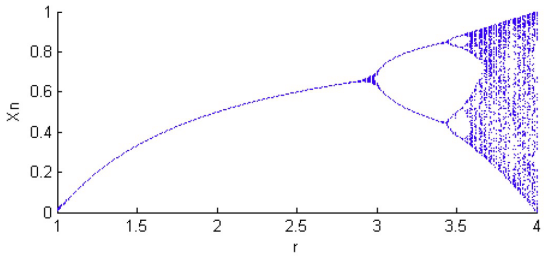

Fig.4: *Bifurcation diagram of the logistic map.*

Image encryption based on chaos can be divided into full encryption and partial encryption. Moreover, with respect to encryption ciphers, the two encryption methods are chaotic block cipher and chaotic stream cipher. In the proposed algorithm we have used partial encryption on chaotic block cipher.

5. THE PROPOSED ALGORITHM

The step by step procedure of the partial image encryption as well as decryption process by logistic chaotic map is similar to that in paper [18]. The different groups of non-overlapping intervals of $f(x_n)$ values, based on which 15 DCT coefficients from each block are chosen for encryption. Each of these is first converted to binary sequence of 24 bits. Here 11 bits are allocated for integer part and rest is for functional part. The different encryption operations that are performed are in Table 1 as in figure 5 as the over all process. The SVD based watermarking and detection algorithm used is our previously published method as in [12] and [13]. The image is divided in three matrices by singular value decomposition, two orthogonal and one eigen value matrix. This is the watermarking algorithm W_{ALGO}. This is followed up by the adding of the logo and the reverse SVD process to obtain watermarked image. The watermark detection scheme D_{ALGO} is the reverse of the W_{ALGO}.

The original image is extracted in three channels R, G and B as shown in figure 6 using the WALGO which is the SVD based watermarking algorithm block applied on each channel. After extraction it undergoes DCT and 15 coefficients are taken as in [18]. Encryption operations are done over those values after converting it to binary values with different

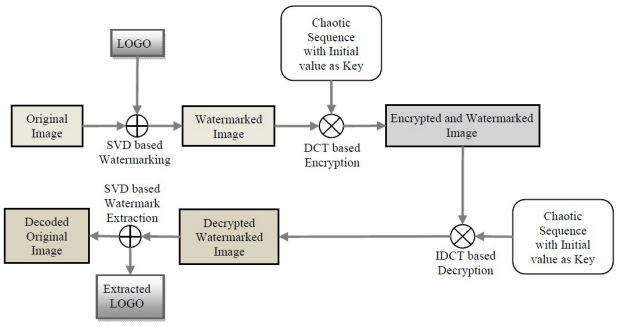

Fig.5: *The Proposed Algorithm Flow Diagram.*

operations explained in Table1. IDCT is performed to get the encrypted image.

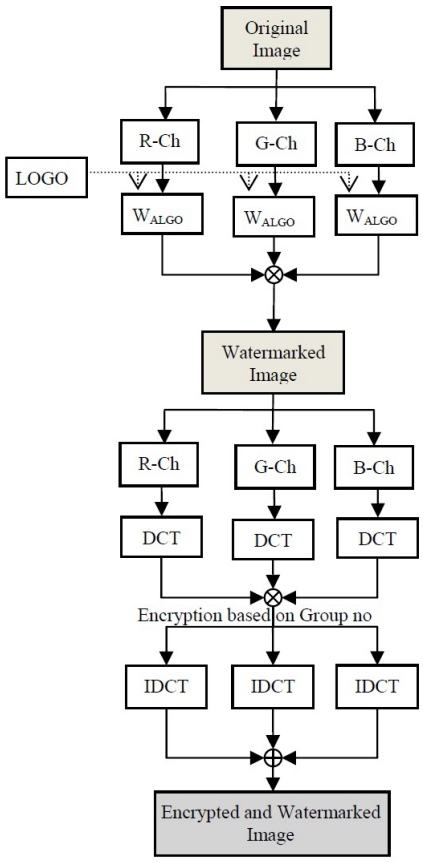

Fig.6: *Flow chart from original image to encrypted image.*

Decryption is the reverse process of encryption where encrypted image is taken as input and channels are extracted, which undergoes DCT. Decryption operations are performed as explained in table1. Then IDCT (inverse discrete cosine transform) is done to get the decrypted image using the DALGO which is the watermark detection algorithm as in figure 7.

Table 1: *Different groups of non-overlapping intervals of $f(x_n)$ values and corresponding operations for image encryption and decryption.*

G No.	Interval of $f(x_n)$ values	Operation of Encryption/Decryption
1	0.10-0.13, 0.34-0.37, 0.58-0.62	Encryption/ Decryption $T(1:8)\oplus K_1$, $T(9:16)\oplus K_2$, $T(17:24)\oplus K_3$
2	0.13-0.16, 0.37-0.40, 0.62-0.66	Encryption/ Decryption $T(1:8)\oplus K_2$, $T(9:16)\oplus K_3$, $T(17:24)\oplus K_4$
3	0.16-0.19, 0.40-0.43, 0.66-0.70	Encryption/ Decryption $T(1:8)\oplus K_3$, $T(9:16)\oplus K_4$, $T(17:24)\oplus K_5$
4	0.19-0.22, 0.43-0.46, 0.70-0.74	Encryption/ Decryption $T(1:8)\oplus K_4$, $T(9:16)\oplus K_5$, $T(17:24)\oplus K_6$
5	0.22-0.25, 0.46-0.49, 0.74-0.78	Encryption/ Decryption $T(1:8)\oplus K_5$, $T(9:16)\oplus K_6$, $T(17:24)\oplus K_7$
6	0.25-0.28, 0.49-0.52, 0.78-0.82	Encryption/ Decryption $T(1:8)\oplus K_6$, $T(9:16)\oplus K_7$, $T(17:24)\oplus K_8$
7	0.28-0.31, 0.52-0.55, 0.82-0.86	Encryption/ Decryption $T(1:8)\oplus K_7$, $T(9:16)\oplus K_8$, $T(17:24)\oplus K_9$
8	0.31-0.34, 0.55-0.58, 0.86-0.90	Encryption/ Decryption $T(1:8)\oplus K_9$, $T(9:16)\oplus K_1$, $T(17:24)\oplus K_2$
9	0.00-0.10, 0.90-1.0	Encryption/ Decryption $T(1:8)\oplus K_1$, $T(9:16)\oplus K_3$, $T(17:24)\oplus K_5$

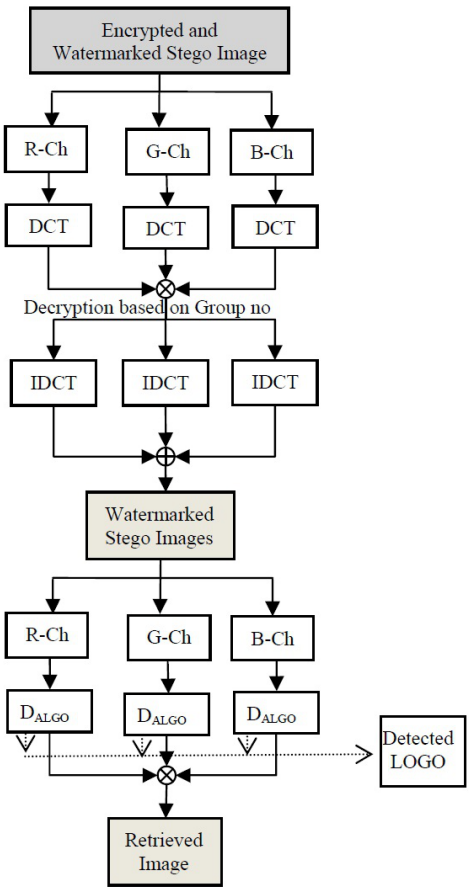

Fig.7: *Flow chart from encrypted image to decrypted image.*

6. EXPERIMENTAL RESULT

In this section the results are obtained by analyzing the 16 standard test images with our proposed algorithm. The 16 standard images used are as in figure 8. Out of these 16 colored images, 8 were of size 256×256 and rest 512×512. Here the respective planes of the colored image, i.e. Red, Green and Blue, were analyzed with respect to their encrypted counterparts after watermarking. Here the 32×32 binary logo shown in figure 9 was watermarked in all the three channels using SVD algorithm as in figure 6. Similarly the logo is detected for the individual channels as in figure 7.

In figure 10, above the channel-wise watermarked original images, along with their encrypted and decrypted versions are shown. Here the grey scale version of the red, green and blue channels are shown. The combination of the three watermarked channels produces the colored watermarked image, along with the encrypted and decrypted image is shown in figure 11.

Here as per the table 2 it can be seen that the respective channel correlations with original verses the watermarked-encrypted images for each channel is highly un-correlated. But on decryption substantial amount of correlation is achieved. While after decoding and detecting the logo the correlation is high for images of 512×512 size where as for the 8 images of size 256×256 the correlation even though not exactly 100% but it is nevertheless high enough. This phenomenon is mainly due to the fact that the percentage of payload distribution is higher in the larger images.

This proposed work also enhances the security as a key of 80 bit is used for encryption of the watermarked image. This thereby enhances the security even better than the traditional simple watermarking algorithms as well as encryption schemes when used alone.

7. CONCLUSION

The paper presents a combined scheme of encryption and watermarking to provide high security in copy protection as well as to facilitate secret communication. The images were watermarked using the SVD based algorithm, then encrypted with chaotic logistic map technique. A 32×32 binary logo was embedded in all 3 channels of the colored images (R, G and B channel). The logo was embedded in all 3 channels and later reconstructed by averaging all the three retrieved logos. Thereby three pronged detection can be achieved from each channel. Thus, unless the unauthorized action specific attacks are effecting all three channels the logo can be detected properly. Moreover the usage of SVD helps in gaining robustness as well as ease in hardware implementation. Nine different XOR operations were performed on the first 15 coefficient of DCT undergone on 8×8 blocks.

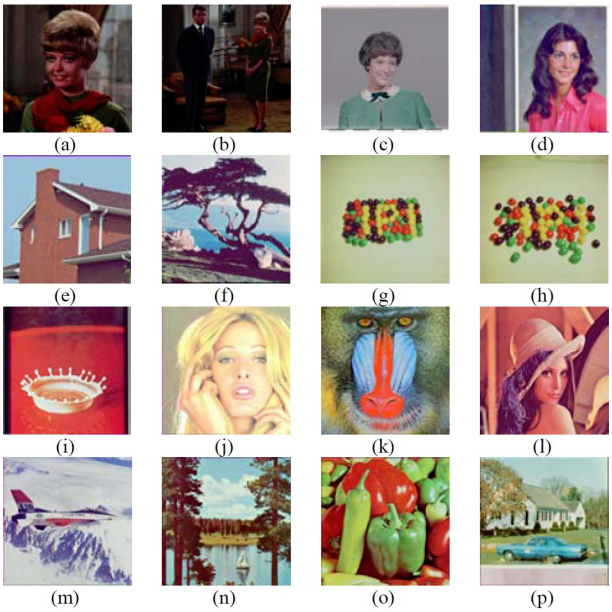

Fig.8: *(a) Girl 1,(b) Couple,(c) Girl 2, (d) Girl 3, (e) House, (f)Tree, (g)Jelly beans 1, (h) Jelly beans 2, (i) Splash, (j) Girl (Tiffany), (k) Mandrill (a.k.a. Baboon), (l) Girl (Lena, or Lenna), (m) Airplane (F-16), (n) Sailboat on lake, (o) Peppers, and (p) Car.*

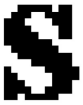

Fig.9: *32×32 binary logo (watermark).*

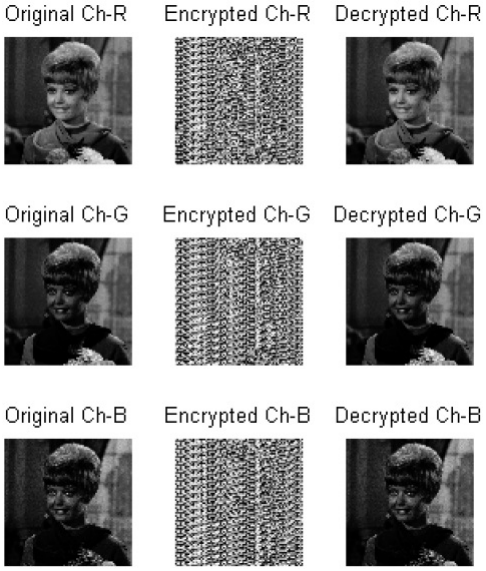

Fig.10: *Channel wise watermarked original images, along with their encrypted and decrypted versions.*

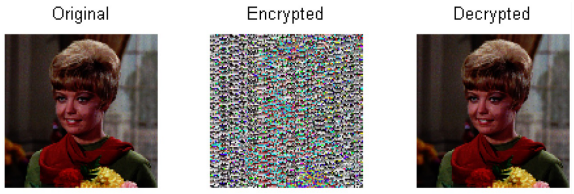

Fig.11: *Watermarked-colored original, encrypted and decrypted images.*

Table 2: *The correlation coefficient based analysis with the 16 test images with respect to their original encrypted original and decrypted versions along with that of detected logo.*

Sl No.	Correlation with Encrypted			Correlation with Decrypted			Correlation of decrypted Logo
	R	G	B	R	G	B	
1	-0.047661	-0.033148	-0.041904	1	1	1	0.99161081
2	-0.030161	-0.033676	-0.036935	1	1	1	0.99161081
3	-0.041636	-0.036085	-0.03102	1	1	1	0.99161081
4	-0.058696	-0.062438	-0.041636	1	1	1	0.99161081
5	-0.031578	-0.043715	-0.051842	1	1	1	0.99161081
6	-0.053562	-0.078678	-0.058918	1	1	1	0.99161081
7	-0.022283	-0.037851	-0.049137	1	1	1	0.99161081
8	-0.035016	-0.051723	-0.04836	1	1	1	0.99161081
9	-0.038566	-0.061423	-0.042504	1	1	1	1
10	-0.030936	-0.024037	-0.030395	1	1	1	1
11	-0.055317	-0.053797	-0.068249	1	1	1	1
12	-0.047038	-0.054763	-0.031643	1	1	1	1
13	-0.042893	-0.046269	-0.026313	1	1	1	1
14	-0.045153	-0.080725	-0.080505	1	1	1	1
15	-0.038936	-0.068425	-0.046468	1	1	1	1
16	-0.049926	-0.050005	-0.060273	1	1	1	1

This combined technique has been performed on 16 standard color images of different types. It was found that the algorithm is quite efficient and provides security from the secrecy and authentication point of view. Chaotic special property of sensitivity towards initial conditions leads to high password strength and higher resistance to brute-force attack.

References

[1] N.K. Pareek, V. Patidhar and K.K. Sud, "Image Encryption Using Chaotic Logistic Map," *Image and Vision Computing*, Vol. 24, pp. 926–934, Sep. 2006.

[2] M.K. Mandala, G.D. Banika, D. Chattopadhyaya and D. Nandib, "An Image Encryption Process based on Chaotic Logistic Map," *IETE Technical Review*, Vol.29, pp. 395–404, Sep. 2012.

[3] S. Zhaopin, G. Zhang, and J. Jiang, "Multimedia security: a survey of chaos-based encryption technology", *INTECH Open Access Publisher*, Mar. 2012.

[4] A. Kahate, *Cryptography and Network Security*, 2nd ed., TATA McGRAW HILL, 2009, pp. 38–77.

[5] S. Lian, *Multimedia Content Encryption: Tech-*

niques and Application, CRC Press, 2008, pp 43–85.

[6] S. Lian, J. Sun, D. Zhang and Z. Wang, "A Selective Image Encryption Scheme Based on JPEG2000 Codec," A in *Multimedia Information Processing - PCM 2004, Lecture Notes in Computer Science*, Vol. 3332, pp. 65–72, Jan. 2005.

[7] K.C.Ravishankar and M.G.Venkateshmurthy, "Region Based Selective Image Encryption," *International Conference on Computing & Informatics, ICOCI '06*, pp. 1–6, 2006.

[8] M. Saikia and S. Majumder, "Spread Spectrum Embedding of Colluder Traceable Codeword in Multimedia," *Emerging Applications of Information Technology (EAIT), 2011 Second International Conference on*, pp.190–193, Feb. 2011.

[9] M. Saikia, S.J. Bora and Md. A. Hussain, "A Review on Applications of Multimedia Encryption," in *national conference on Network Security- issues, challenges and Techniques*, at Tezpur University, pp.30–33, Jan. 2012.

[10] N.S. Kulkarni, B. Raman, and I. Gupta, "Selective Encryption Of Multimedia Images," *XXXII National Systems Conference, NSC 2008*, Dec. 2008.

[11] B. Prasad and K. Mishra, "A Combined Encryption Compression Scheme Using Chaotic Maps," *Cybernetics and Information Technologies*, Vol. 13, No. 2, pp. 75–81, Jul. 2015

[12] S. Majumder, T. S. Das, V. H. Mankar and S. K. Sarkar, "SVD and Error Control Coding based Digital Image Watermarking," *Advances in Computing, Control, & Telecommunication Technologies, 2009. ACT '09. International Conference on*, pp. 60–63, Dec. 2009.

[13] M. Saikia, S. Majumder, T. S. Das, Md. A. Hussain and S. K. Sarkar, "Coded Fingerprinting Based Watermarking to Resist Collusion Attacks and Trace Colluders," *Advances in Computer Engineering (ACE), 2010 International Conference on*, pp.120–124, Jun. 2010.

[14] S. Majumder and T. S. Das, "Watermarking of Data Using Biometrics," *Handbook of Research on Computational Intelligence for Engineering, Science, and Business*, IGI Global, 2013., pp. 623-648, Jul. 2015.

[15] S. Majumder, K Jilen Kumari Devi and S. K. Sarkar, "Singular value decomposition and wavelet-based iris biometric watermarking," in *IET Biometrics*, Vol. 2, pp. 21 - 27, Mar. 2013.

[16] S. Majumder, M. Saikia, S. Sarkar and S. K. Sarkar, "A Novel SVD and GEP Based Image Watermarking," *Proceedings of the 48th Annual Convention of Computer Society of India- Vol II. Advances in Intelligent Systems and Computing*, Vol. 249, pp. 601–608., 2014.

[17] A. K. Shaw, S. Majumder, S. Sarkar and S. K. Sarkar, "A novel EMD based watermarking of fingerprint biometric using GEP," *Procedia Technology, in the First International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA-2013)*, Vol. 10, pp. 172–183, Sep. 2013.

[18] N. Hazarika and M. Saikia, "A Novel Partial Image Encryption using Chaotic Logistic Map," *Signal Processing and Integrated Networks (SPIN), 2014 International Conference on*, pp 231–236, Feb. 2014.

Monjul Saikia has been serving as an Assistant Professor in the department of Computer Science and Engineering, NERIST (North Eastern Regional Institute of Science and Technology) a Deemed University under the Govt. of India, in Arunachal Pradesh, India since July 2007. He has completed his Masters of Technology from the Department Computer Science and Engineering, NERIST in the year of 2011. He did his Bachelor of Engineering from Jorhat Engineering College, Jorhat Assam, in 2005 in Computer Science discipline. His major research interests include Information Security, Cryptography, Image and Video Processing, VLSI etc. He is a member of professional societies like IEEE, CSI (India), IEI (India) and ISTE (India).

Swanirbhar Majumder has been serving as an Assistant Professor in the department of Electronics and Communication Engineering of NERIST (North Eastern Regional Institute of Science and Technology) a Deemed University in Arunachal Pradesh, India since July 2006. He has completed his PhD thesis in the field of Image and signal processing from Dept of ETCE, Jadavpur University in 2015. He had done his M.Tech from the Dept of Applied Physics, University of Calcutta in 2006 after attaining his B.Tech, Diploma and ITI from NERIST then under the North Eastern Hill University, Shillong in the years 2004, 2002 and 2000 respectively in the field of Electronics and Communication Engg. His interests include Biomedical and Image signal processing, soft Computing and Embedded Systems. He is part of professional societies like IEEE, ACM, IAENG, IEI (India), IETE (India),and ISTE (India).