International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Security of Information Using Cryptography and Image Processing

Mrunalinee Patole[1], Sheela A Bankar[2]

[1]PG Coordinator Comp, RMDSSOE, Maharashtra, India

[2]ME Second Year, COMP, RMDSSOE, Maharashtra, India

Abstract: ***In this paper we propose a same technique of sending confidential information using encryption and data hiding concept with different encryption algorithms, that is for image encryption we use AES algorithm and for data encryption we use Twelve Square cipher substitution algorithm, and try to improve the security mechanism. With plain text data we also consider the confidential audio and video data for embedding purpose. This work also proposes a scheme for separable reversible data hiding in encrypted image which is remove the drawback of non separable reversible data hiding in encrypted image.***

Keywords: Image encryption, Decryption, twelve square cipher, reversible data hiding, non-separable reversible data hiding**.**

1. Introduction

Now a day's signal processing with encryption is interesting research topic. For day to day work or transaction of any kind of data we are using computerized system , so the security is most important factor and considering this the proposed system tries to solve the problem of security .Fig 1. shows the proposed system architecture which explain all the steps in the proposed system .This proposed system is used to remove the drawback of non-separable reversible data hiding in encrypted image system shown in Fig 2. by separating all the different cases at the receiver side which is known as Separable Reversible Data Hiding in Encrypted image [1].

2. Literature Survey

Since the start of internet, one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret.

Unfortunately it is sometimes not enough to keep the contents of the message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this is called steganography. The basic concept of system is taken from [1]. Image is encrypted using simple XOR method but instead of that we add a standard AES algorithm for image encryption. AES algorithm has more security as compare to other algorithm.

To encrypt the image AES algorithm can be used because AES. Based on 128-bit blocks, with 128-bit a key which removes the weakness in DES. This algorithm gives the lot of flexibility and security to the implementers. It also stands up well against cryptanalysis attack. Also this algorithm works well with modern processors [17].From [2] we have taken a 12 square data encryption algorithm. This will give us more security for our data. The twelve-square cipher encrypts alphabets, digits and special characters and thus is less susceptible to frequency analysis attacks. In [11] to extract the embedded data first we have to decrypt the image but in our proposed system without decrypting image we can get the embedded data. Using [3] solve the problem of transmitting redundant data over an insecure, bandwidth-constrained communications channel by reversing the order of the steps, i.e., first encrypting and then compressing the encrypted source[3,4]. In [5] Author presented the lossy compression method. There are a number of works on data hiding in the encrypted domain. In [6] author represent a buyer–seller watermarking protocol. In [7] author presents the Okamoto-Uchiyama encryption method for fingerprinting which will improves the enciphering rate. In [8] author introduces the composite signal representation mechanism. The intraprediction mode, motion vector difference and signs of DCT coefficients are encrypted, while a watermark is embedded into the amplitudes of DCT coefficients [9,10].Most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain [12-16]. But, in some applications, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. And it is also hopeful that the original content should be recovered without any error after image decryption and message extraction at receiver side

3. Implementation Details

In proposed system first encrypt the image then instead of just hiding the data into the encrypted image first encrypt the data also and then hide/embedded data into encrypted image and then send it to the receiver. To encrypt the image system used standard AES algorithm and to encrypt the text data used twelve square substitution cipher algorithm. By using above two algorithms system provided more security to data. Fig. 3 shows the block diagram of three cases at the receiver side each and every case is independent of each other if receiver has data hiding key and data encryption key he will get the original data but not the original image .If he has image encryption key he will get the original image

without original data and if he has all the keys he will get the original data as well as original image. To implement all the algorithms

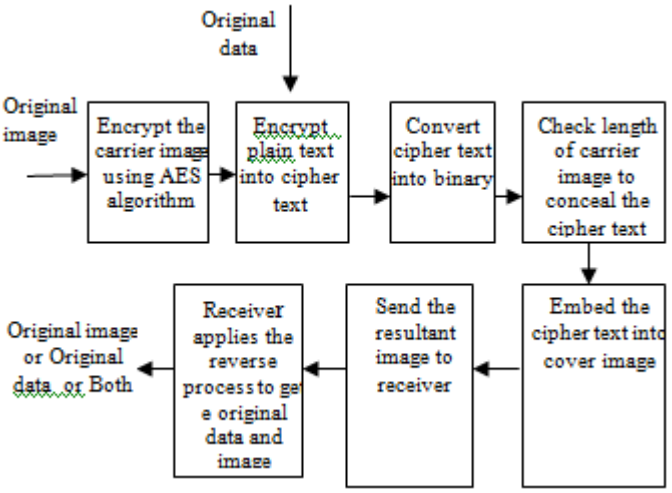

Figure 1: Sketch of proposed system architecture which are included in this proposed system Java programming is used.

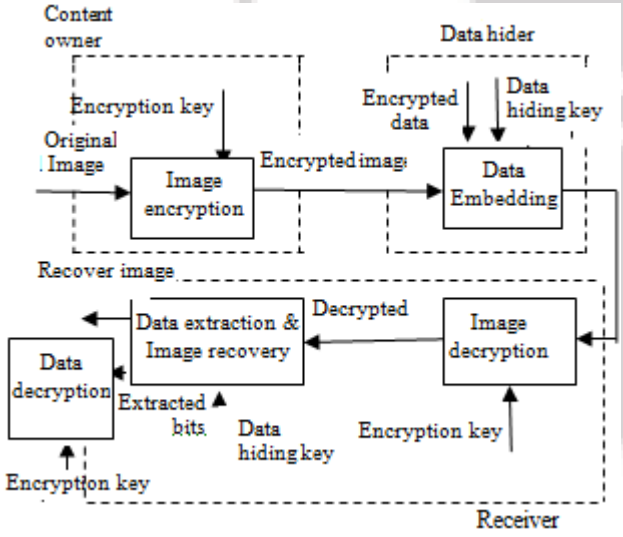

Figure 2: Sketch of non-separable reversible data hiding in encrypted image

3.1 AES algorithm

The AES algorithm uses a round function that is composed of four different byte oriented transformations:

1) byte substitution using a substitution table (s box)
2) shifting rows of the State array by different offsets
3) mixing the data within each column of the State array, and
4) Adding a Round Key to the State.

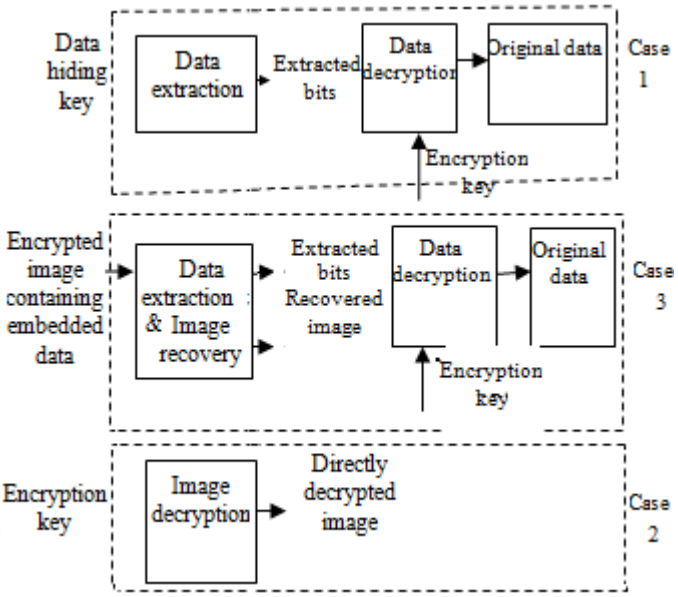

Figure 3: Three cases at receiver side of the proposed scheme

3.2 Twelve Square Substitution Cipher Algorithm

1) The plain text is read from left to right. If the character is an alphabet it refers to table-1, otherwise if it is a number or a special character it refers to table-2.
2) While scanning the plain text the first alphabet's plain text is in square-1 and its cipher is in same row and column location of square-4.
3) The second alphabet, its plain text is in square-2 and cipher text is in same row and column location of square 5.
4) The third alphabet, its plain text is in square-3 and cipher text is in same row and column location of squar6.
5) Similarly fourth alphabet corresponds to square-1and square-4, 5th alphabet corresponds to square-2 and square- 5,6th alphabet corresponds to square-3 and square-6 and so on.
6) Same method is applied for special characters and numbers.

Table 1: Plain text and cipher text (alphabets)

Square 1	Square-2	Square-3
a b c d e	f g h i j	k l m n o
f g h i j	k l m n o	p r s t u
k l m n o	p r s t u	v w x y z
p r s t u	v w x y z	a b c d e
v w x y z	a b c d e	f g h i j
Square-4	**Square-5**	**Square-6**
g m r i t	a b c d e	a b c d e
a b c d e	f h j k l	f h j k l
f h j k l	g m r i t	n o p s u
n o p s u	n o p s u	v w x y z
v w x y z	v w x y z	g m r i t

3.3 Data Embedding

Now we have image in encrypted pixel. Image size **N1 × N2.** Total no of pixel **N= N1 × N2.** In this phase, some parameters are embedded into a small number of encrypted pixels **NP** and the LSB of the other encrypted pixels are compressed to create a space for accommodating the additional data and the original data at the positions occupied by the parameters.

Table 2: Plain text and cipher text (digits and special characters)

Square 7	Square-8	Square-9
0 1 2 3 4 5 6 7 8 9 ` ~ ! @ # $ % ^ & * ( ) _ - + = { [}] ; : “ ‘ \ | < , > . ? /	7 8 9 ` ~ ! @ # $ % ^ & * ( ) _ - + = { [}] ; : “ ‘ \ | < , > . ? / 0 1 2 3 4 5 6	# $ % ^ & * ( ) _ - + = { [}] ; : “ ‘ \ | < , > . ? / 0 1 2 3 4 5 6 7 8 9 ` ~ ! @
Square-10	**Square-11**	**Square-12**
0 6 ! & + ; < 1 7 @ * = : , 2 8 # ({ “ > 3 9 $) [‘ . 4 ` % _ } \ ? 5 ~ ^ -] | /	1 7 @ * = : , 2 8 # ({ “ > 0 6 ! & + ; < 3 9 $) [‘ . 4 ` % _ } \ ? 5 ~ ^ -] | /	1 7 @ * = : , 2 8 # ({ “ > 3 9 $) [‘ . 4 ` % _ } \ ? 5 ~ ^ -] | / 0 6 ! & + ; <

3.4 Data Extraction and Image Recovery

According to the Fig.3 at a receiver side there are three different cases. Depend on the availability of the keys at the receiver side receiver will get the original data and original image.

3.5 Operating Environment

Software Requirement:
Technology: jdk-6u21-windows-i586
OS: Windows
Tool: Netbean IDE 7.3

Hardware Requirement:
Processor: At Least Pentium Processor

4. Mathematical Model

The mathematical model for proposed system is as follows:
Input= Original Image and Original Data
Process=AES algorithm, Twelve square substitution cipher algorithm Data embedding process.

a) Module 1: AES algorithm

1. Let I be the input carrier image
2. A=Byte array to store image pixel by pixel
State= group of 16 bytes. round = 1 to10 perform
a) SubBytes(state)
The SubBytes() transformation is a non-linear byte substitution that operates independently on each byte of the State using a substitution table (S-box).
b) ShiftRows(state)

$$s'_{r,c} = s_{r,(c+\,shift\,(r,\,Nb))\bmod Nb} \text{ for } 0 < r < 4 \text{ and } 0 \le c < \boldsymbol{Nb}, \quad (1)$$

c) Mix Columns (state)
$s'(x \quad a(x \;;\; 2\,5 \quad s(x)$: where a(x) is fix matri (2)
d) AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
W=roundkey, State=128 bit represented by Nb

b)Module 2: Twelve Square Substitution cipher algorithm

Using table1 and table2 according to the corresponding square find out the cipher value of a given plain text.

c) Module 3 : Data Embedding

1) Image size = **N1 × N2**
2) **(N-NP)** pixels are divided into no of groups each of which contains **L** pixels
3) **M** = least significant bits of the **L** pixels denoted as **B(k,1),B(k,2),….,B(k,M . L) k= group index**
4) **G = [$I_{M.L-S}$, Q]**

I (M.L-S) × (M.L-S) identity matrix , Q (M.L-S)× S binary matrix derived from data hiding key. **S** is small positive integer.

5) $$\begin{bmatrix} B'(k,1) \\ B'(k,2) \\ \vdots \\ B'(k,ML) \end{bmatrix} = G. \begin{bmatrix} B(k,1) \\ B(k,2) \\ \vdots \\ B(k,ML) \end{bmatrix} \quad (3)$$

*[B'(k,M . L-S+1) , B'(k,M . L-S+2), B'(k,M . L-S+2)…. B'(k,M . L)]*of each group be the original LSB and additional data to be embedded.

5. Experimental Result

The test image sunset sized 800 × 600 shown in Fig. 4 was used as the original image in the experiment. AES algorithm was used for image encryption.

Figure 4: Original image

To encrypt the plain text data or audio data or video data we used Twelve Square Substitution Cipher algorithm

please send original document on or before 20 may

Figure 5: The secret information to be sent

please send original document on or before 20 may

(a)

nhzgrz pzdi lhdbikvb ilxujzki ek lh mzglmz !5 jvs

Figure 6: Cipher text to be embedded

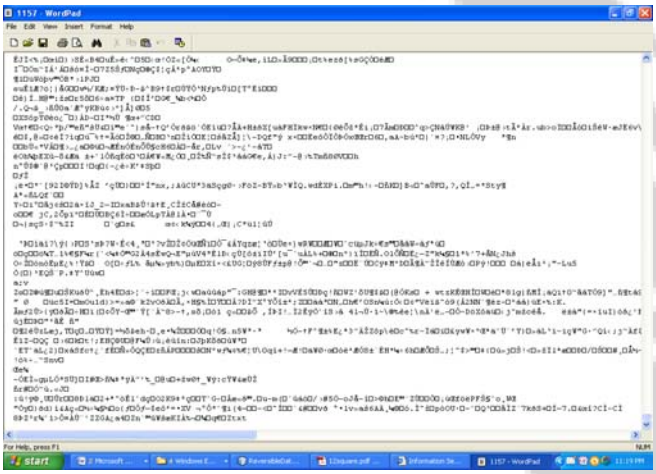

Figure 7: The resultant encrypted image to be transmitted (after embedding) .open with wordpad.

(b)

Figure 8: (a), (b) The retrieved information from the image or directly decrypted image at the receiver

Figure 9, 10, 11 are the snapshots of the screen at sender and receiver side for audio data

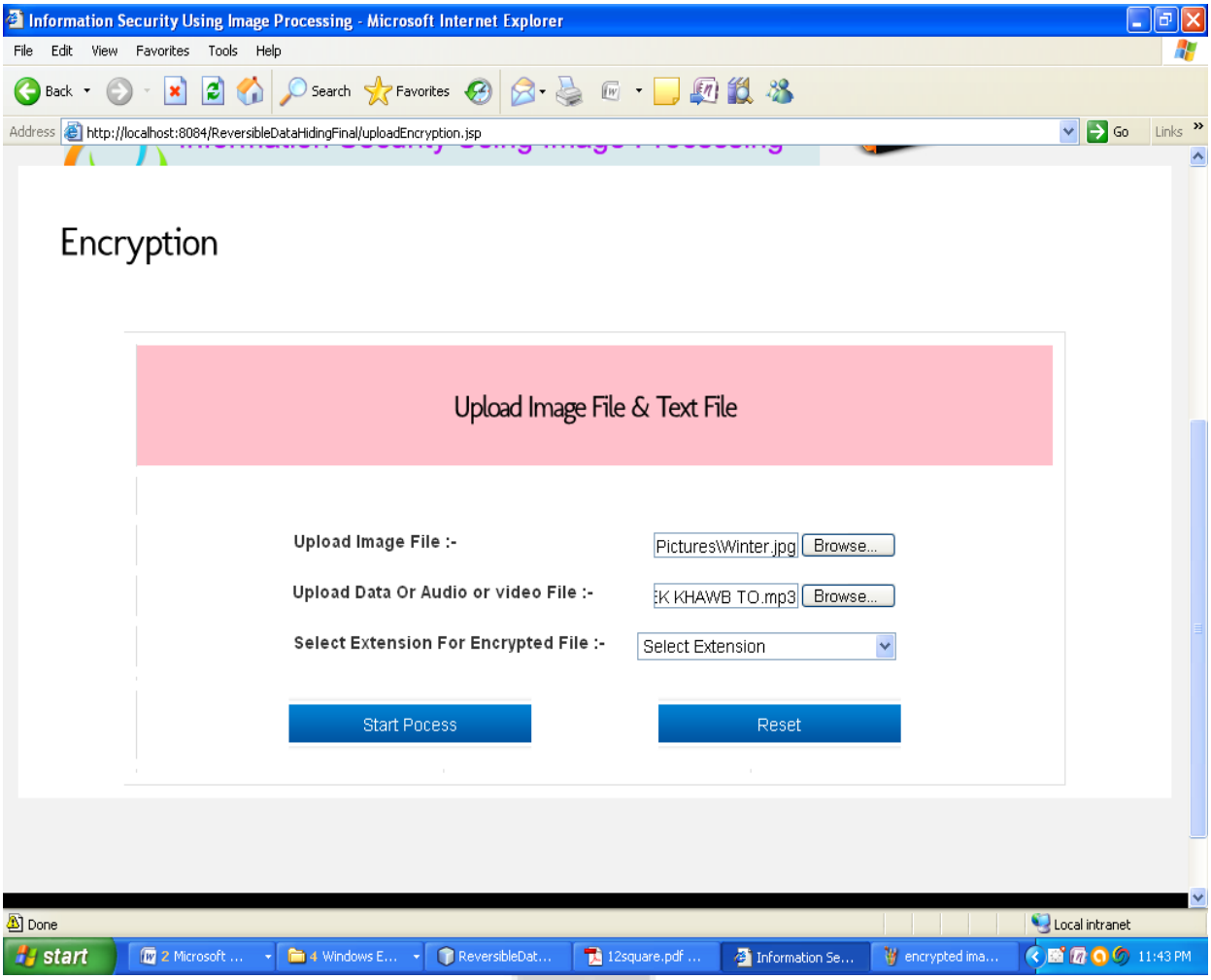

Figure 9

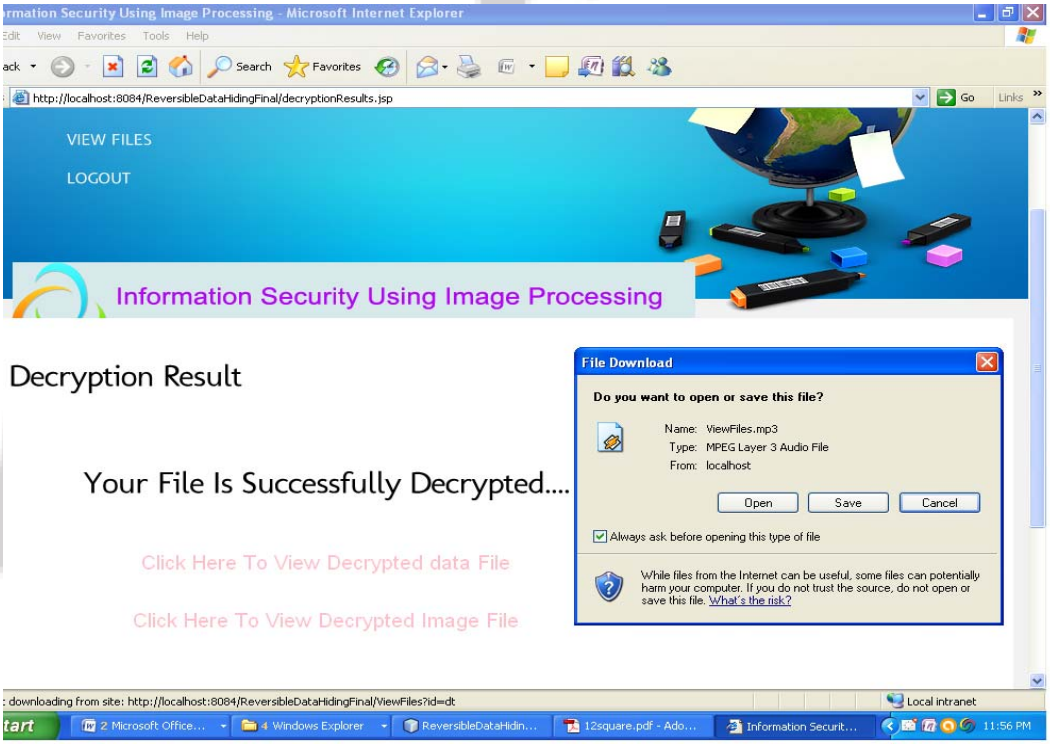

Figure 10

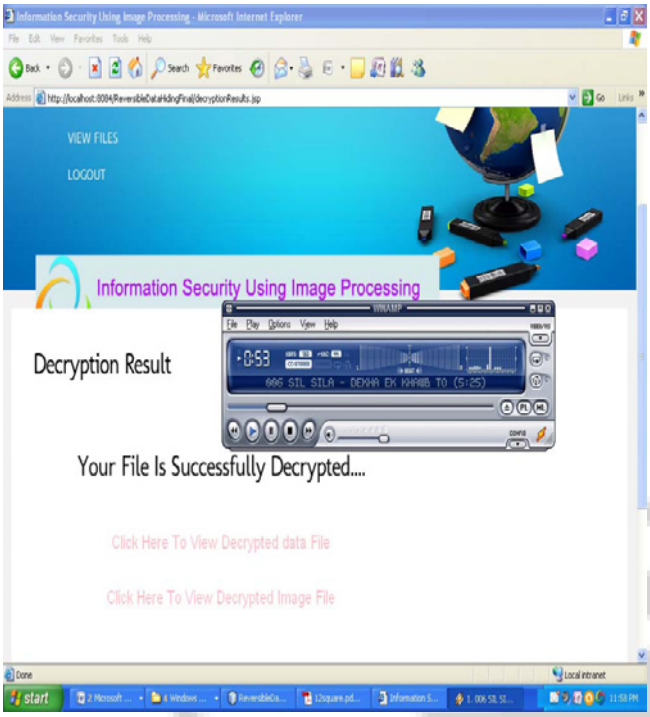

Figure 11

6. Conclusion

In this paper we remove the drawback of non separable reversible data hiding in encrypted image using separable reversible data hiding in encrypted image. In the proposed system if the receiver has only the data-hiding key get the embedded parameters and get the extracted bits but in encrypted version. With the help of encryption key receiver get the original data.

Any attacker without the data-hiding cannot extract the embedded data. Using the data hiding key the receiver successfully extract the embedded data, but cannot get any information about the original image content without image encryption key. In the second case the receiver has the encryption key but does not know the data-hiding key. Clearly, cannot obtain the values of parameters and cannot extract the embedded data. But, the original image content can be roughly recovered by decrypting the image. And finally in the third case if the receiver has all the keys that is image encryption, data encryption, data hiding key he will get the original data as well as original image.

In this paper we use standard AES algorithm for image encryption and Twelve Square Substitution Cipher algorithm for data encryption. With the help of these two algorithms this system is successfully embedded audio and video data in encrypted image and send to the receiver. In the future we can concentrate on different type of image encryption and data embedding algorithms to improve the accuracy as well as security.

7. Acknowledgement

This is a great pleasure & immense satisfaction to express my deepest sense of gratitude & thanks to everyone who has directly or indirectly helped me in completing my dissertation work. A dissertation work of such a great significance is not possible without the help of several people, directly or indirectly. First and foremost I have immense happiness in expressing my sincere thanks to my guide, Prof. Mrunalinee Patole ME-coordinator of Computer Engineering Department for his continuous encouragement and for developing a keen interest in this field. I feel a deep sense of gratitude to Prof. D.N. Rewadkar, HOD Computer Engineering Department for his valuable suggestions, co-operation and continuous guidance. It's my pleasure to thank Dr.P.M.Patil, Principal, who is always a constant source of inspiration. I am very much thankful to all my faculty members whose presence always inspires me to do better. No words are sufficient to express my gratitude to our parents for their unwavering encouragement.

References

[1] Xinpeng Zhang "Separable Reversible Data Hiding in Encrypted Image" *IEEE Transactions on Information Forensics And Security*, Vol. 7, No. 2,pp.826-832 April 2012

[2] Gandharba Swain, Saroj Kumar Lenka "Steganography Using the Twelve Square Substitution Cipher and an Index Variable" 978-1- 4244-8679-3/11/$26.00 ©

[3] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. Signal Process.* vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[4] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Image Process.*, vol. 19, no. 4 pp. 1097–1102, Apr. 2010.

[5] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Trans. Inform. Forensics Security*, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[6] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol," *IEEE Trans. Image Process.*, vol. 10, no. 4, pp. 643–649, Apr. 2001.

[7] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2129–2139, Dec. 2005.

[8] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and Watermarking in video compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 17, no. 6, pp. 774–778, Jun. 2007.

[9] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar domain," *Sign Processing: Image Commun.*, vol. 26, no. 1, pp. 1–12, 2011.

[10] D. Kundur and K. Karthik, "Video fingerprinting and encryption Principle for digital rights management," *Proceedings IEEE*, vol. 92, no. 6, pp. 918–932, Jun. 2004.

[11] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[12] Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.,* vol. 13, no. 8, pp. 890– 896, Aug. 2003.
[13] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.,* vol. 16, no. 3, pp. 354– 362, Mar. 2006.
[14] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized- LSB data embedding," *IEEE Trans. Image Process.*, vol. 14, no. 2, pp. 253–266, Feb. 2005.
[15] W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, "A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification," *Signal Process.*, vol. 90, pp. 2911–2922, 2010.
[16] C.-C. Chang, C.-C. Lin, and Y.-H. Chen, "Reversible data- embedding scheme using differences between original and predicted pixel values," *IET Inform. Security*, vol. 2, no. 2, pp. 35–46, 2008. 2011 IEEE
[17] Kahate A, 2012, CRYPTOGRAPHY *AND NETWORK SECURITY, Tata McGraw Hill Education Private Limited, 541pp*

Author Profile

Prof. Mrunalinee Patole received the B.E degree in computer from the university of Pune India, in 2007 and the M.E. degree in computer from the University of Pune India, in 2012.she is currently working as Assistant professor in RMD Sinhgad School of Engineering Pune, India

Sheela Bankar received the B.E. degree in computer from the University of Pune India, in 2000 and she is currently working toward the M.E. degree in computer from the Pune University, India