Advanced Partial Image Encryption using Two-Stage Hill Cipher Technique

Panduranga H T
University of Mysore
Dept. of Studies in Electronics
PG-Center Hemagangothri-Hassan
Karantaka, India

Naveen Kumar S K
University of Mysore
Dept. of Studies in Electronics
PG-Center Hemagangothri-Hassan
Karantaka, India

ABSTRACT
Information security is a fast growing research field which includes numerous problems in it. Partial image encryption is one of the important problems in the field of image information security. This paper describes the partial image encryption in two ways using hill cipher technique. First encryption technique uses two slightly different keys to construct two self-invertible matrices, which are used in two different stages to get partially encrypted image. Second encryption technique useone key to construct one self-invertible matrix and it is used in first stage. In second stage same key matrix along with few modification in diagonal values are used to construct another self-invertible matrix which leads to partial image encryption. Reverse process is employed to reconstruct the original image. Experiment is conducted for different images with different combinations of passwords to obtain partially encrypted image.

General Terms
Information security, Image encryption.

Keywords
Partial encryption, hill cipher, carrier image, self-invertible matrix.

1. INTRODUCTION
The rapid growth of technology concerns all scientific research fields including the processing and transmission of digital images. In many fields like military, medical, industry, multimedia, communication or even personal, millions of images are stored or transmitted through internet every day. Depending on the application domain, the need to protect these images against unauthorized users has become a challenge.

Conventional Encryption is referred to as symmetric encryption or single key encryption. It can be further divided into categories of classical techniques and modern techniques. A substitution cipher is a method of encryption by which units of plaintext are substituted with cipher-text according to a regular system; the units may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution. The units of the plaintext are retained in the same sequence as in the cipher text, but the units themselves are altered. There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different times in the message— such as with homophones, where a unit from the plaintext is mapped to one of several possibilities in the cipher-text. Hill cipher is a type of monoalphabeticpolygraphic substitution cipher. A novel method of generating self-invertible matrix is proposed which can be used in Hill cipher algorithm [1]. In this paper they try to overcome the drawback of using a random key matrix in Hill cipher algorithm for encryption, where we may not be able to decrypt the encrypted message, if the matrix is not invertible. Also the computational complexity can be reduced by avoiding the process of finding inverse of the matrix at the time of decryption, as we use self-invertible key matrix for encryption [2]. How to adapt certain matrix transformation to create a novel asymmetric block encryption scheme and a scheme is especially useful for encryption of large amounts of data, such as digital images. First, pair of key are given by using matrix transformation; Second, the image is encrypted using private key in its transformation domain; Finally the receiver uses the public key to decrypt the encrypted messages. This scheme satisfies the characters of convenient realization, less computation complexity and good security. Here they are used encryption in DCT domain [4]. A fast chaos-based image encryption system with stream cipher structure is proposed. In order to achieve a fast throughput and facilitate hardware realization, 32-bit precision representation with fixed point arithmetic is assumed [5].Image encryption can also be categorized as full image-encryption [1]-[7] and partial/selective image encryption [8]-[10]. Performance parameters of image encryption algorithms are discussed in [11, 12]. In [8] we developed a new 4 out of 8 code; it is a unique 8 bit code in which each nibble is having 2 ones and two zeros to create a 36 different 8 bit number. We have 26 alphabets and 10 numerals to form 36 alphanumeric characters. These alphanumeric characters are assigned with unique codes of 4 out of 8 codes.

2. OVERVIEW OF IMAGEENCRYPTION USING HILL CIPHER
The idea of the Hill cipher is a simple matrix transformation. Let us consider an arbitrary plaintext string of length l, defined over an alphabet of order n. We divide that plaintext into b blocks of length m, where m is an arbitrary chosen positive integer and $b=[l/m]$. It is noticed that if the length is not a multiple of m, the last plaintext block must be padded with $l\text{-}b_m$ extra characters. Additionally, each character in the alphabet is coded with a unique integer in$\{0,1,\ldots..,n\text{-}1\}$, in other words, all the characters in the alphabet are mapped to the ring Zn.The *b* plaintext blocks can be rewritten as an *mxb* matrix *p* over *Zn* using the one-to-one mapping between the original alphabet and the ring *Zn* explained above. Additionally, an *mxm* matrix k with coefficients in *Zn* must be

chosen as the secret key matrix. According to the above definitions, Hill encryption can be performed by computing.

For encryption:

$$C = Ek(P) = K\ P \bmod n \qquad (1)$$

For decryption:

$$P = Dk(C) = K^{-1}\ C \bmod n \qquad (2)$$

There might be some complications with the procedure outlined above due to the fact that not all matrices *K* have a inverse k^{-1}over *Zn*. In fact, those matrices *K* with determinant 0, or with a determinant that has common factors with the modulus *n*, will be singular over *Zn*, and therefore they will not be eligible as key matrices in the Hill cipher scheme. Furthermore, due to its linear nature, the basic Hill cipher succumbs to known-plaintext attacks. Fig 1 shows the block diagram of hill cipher.

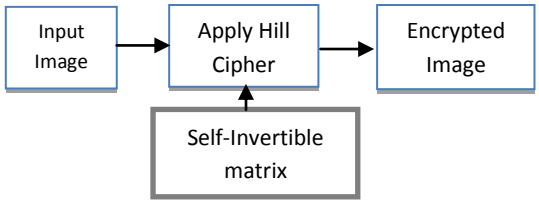


Fig 1: Block diagram of Hill Cipher technique

3. PROPOSED ADVANCED PARTIAL IMAGE ENCRYPTION (APIE) USING SELF – INVERTIBLE MATRIX AS CARRIER IMAGE

Entire encryption process depends on self-invertible matrix and hill cipher. Here key should be of minimum eight characters, in first stage this key is reputedly arranged to form 8x8 matrixes and all its elements are replaced by predefined 4 out of 8 code vales. Then it is used as a basic block in self-invertible matrix generator. Input image is divided in to blocks of 16x16, each block along with self-invertible matrix are undergo hill cipher in first stage to produce an encrypted block. Modification of self-invertible matrix is done by replacing the diagonal values of basic block (8x8) by ASCII value instead of 4 out of 8 code. Resultant block in first stage hill cipher along with a modified self-invertible matrix are undergo second stage hill cypher to get transparent encrypted image. Exact reverse of this proposed encryption process gives decrypted image same as original image. Fig 2 shows the proposed block diagram of advanced partial image encryption. .

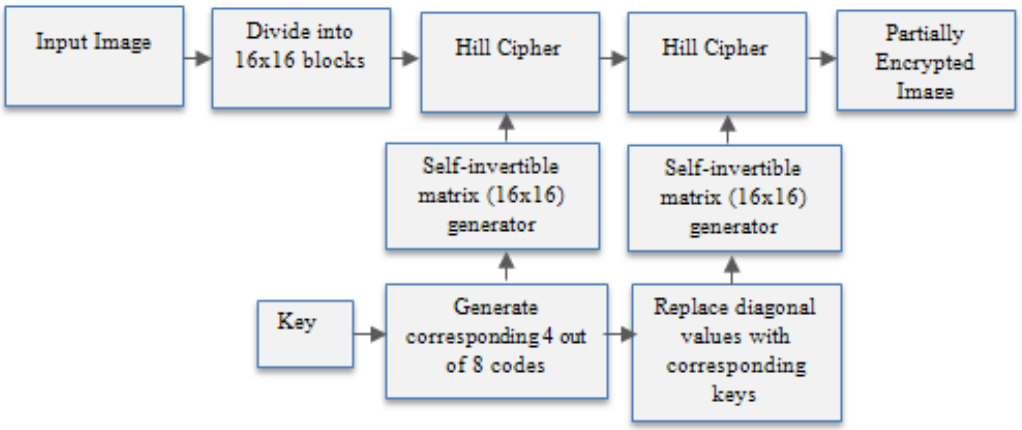


Fig 2. Block diagram of proposed two-stage technique for Advanced PIE.

4. RESULTS AND DISCUSSION

We obtained good results for different images by using proposed APIE method and are tabulated along with the histograms, MSE (Mead Square Error), PSNR (Peak Signal to Noise Ratio), NPCR (Number of Pixel Change Rate) and UACI (Unified Average Changed Intensity). Table-1,2 and 3 shows the result obtained for different input images with changing the diagonal values. In first stage of hill cipher technique all values in the matrix are generated by using 4 out of 8 code. In second stage the values of the diagonal are replaced by ASCII values. From these tables we can understand that due to the change in single value or multiple values in the diagonal of a basic matrix of self-invertible matrix leads to change in Entropy, MSE, PSNR, NPCR and UACI. Improvement in the entropy improve the randomness in the image. As MSE increases PSNR decreases. Increase in the value of NPCR and UACI shows that there is an improvement in the amount of encryption.

If C1 and C2 are original image and encrypted image respectively. Then following parameters are defined as follows.

$$MSE=\frac{1}{M\times N}\sum_{i=1}^{m}\sum_{j=1}^{n}(C1(i,j)-C2(i,j))^2$$

PSNR=$10\log_{10}\left(\frac{255}{MSE}\right)$

NPCR= $\frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%$

$$UACI = \frac{1}{N}\left[\sum_{i,j}\frac{|C(i,j) - C'(i,j)|}{255}\right] \times 100$$

Where D(i,j) defined by the following formula.

$$D(i,j)=\begin{cases}1, & C1(i,j) \neq C2(i,j),\\ 0, & otherwise\end{cases}$$

Table 1. Results obtained by proposed APIE for Lena Image

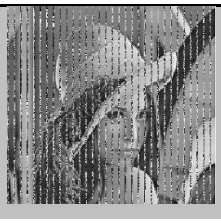
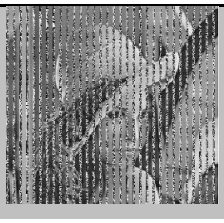
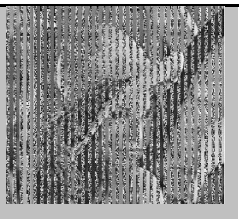
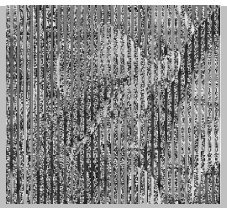
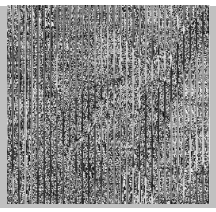
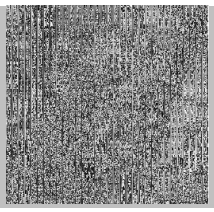
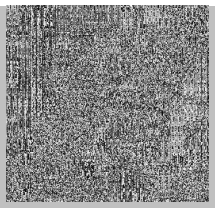
No. of value change	**No change**	**1 diagonal value change**	**2 diagonal value change**	**3 diagonal value change**	**4 diagonal value change**
image					
Entropy	7.5110	7.6518	7.7540	7.8317	7.8923
MSE	0	12.7742	26.7201	40.5705	53.8064
PSNR	0	37.0675	33.8624	32.0487	30.8225
NPCR	0	12.1826	24.3469	36.5753	48.7915
UACI	0	4.775	9.5478	14.3433	19.1339
	No cahnge	5 diagonal value change	6 diagonal value change	7 diagonal value change	8 diagonal value change
image					
Entropy	7.5110	7.9409	7.9722	7.9894	7.9961
MSE	0	67.6390	81.7768	96.8526	111.2226
PSNR	0	29.8288	29.0045	28.2697	27.6689
NPCR	0	61.0596	73.2697	85.4980	97.7417
UACI	0	23.9449	28.7332	33.5286	38.3301

Table 2. Results obtained by proposed APIE for mri brain Image

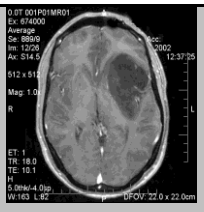
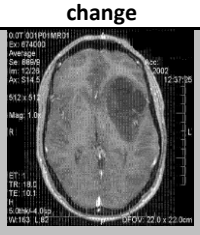
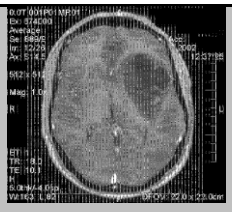
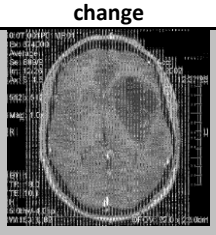
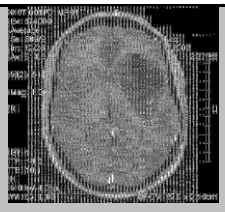
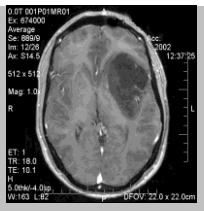
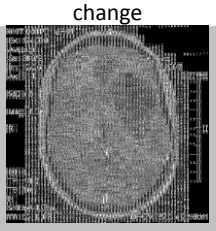
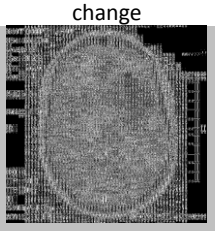
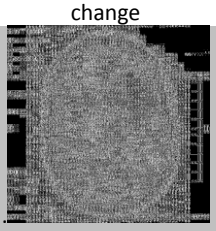
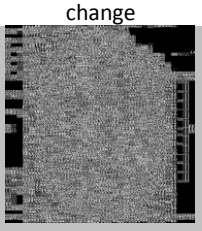
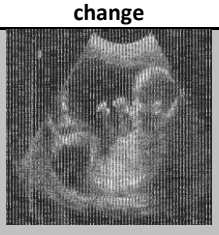
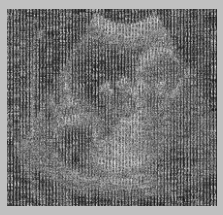
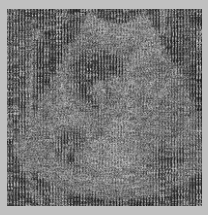
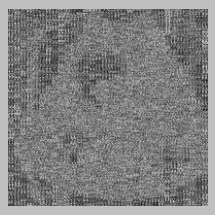
No. of value change	No change	1 diagonal value change	2 diagonal value change	3 diagonal value change	4 diagonal value change
image					
Entropy	6.5628	6.7409	6.8825	7.0078	7.1128
MSE	0	8.3302	16.5142	24.6506	32.8383
PSNR	0	38.9242	35.9522	34.2125	32.9670
NPCR	0	10.36	20.6146	30.7747	40.9714
UACI	0	4.0627	8.0842	12.0685	16.0672
	No cahnge	5 diagonal value change	6 diagonal value change	7 diagonal value change	8 diagonal value change
image					
Entropy	6.5628	7.200	7.2685	7.3204	7.3569
MSE	0	40.5668	48.7681	56.3556	64.2279
PSNR	0	32.0491	31.2494	30.6214	30.0536
NPCR	0	51.2886	61.5593	70.7146	80.8395
UACI	0	20.1132	24.1409	27.7312	31.7018

Table 3. Results obtained by proposed APIE for baby Image

No. of value change	No change	1 diagonal value change	2 diagonal value change	3 diagonal value change	4 diagonal value change
image					
Entropy	6.3942	6.6930	6.9427	7.1482	7.3541

MSE	0	9.5951	15.7438	21.9311	30.3728
PSNR	0	38.3103	36.1597	34.7202	33.3060
NPCR	0	11.5829	23.1583	34.7130	46.2776
UACI	0	4.5423	9.0817	13.6129	18.1481
	No cahnge	5 diagonal value change	6 diagonal value change	7 diagonal value change	8 diagonal value change
image					
Entropy	6.3942	7.5264	7.6738	7.7885	7.8537
MSE	0	37.4032	46.0593	55.7198	62.1443
PSNR	0	32.4017	31.4976	30.6709	30.1968
NPCR	0	57.8712	69.4923	81.1035	92.7299
UACI	0	22.6946	27.2519	31.8053	36.3647

5. CONCLUSION

This paper describes a novel approach for advance partial image encryption method using a dual stage hill cipher technic. From the result we can conclude partial image encryption is enough to secure specific applications like patient information security. By controlling dependency of basic block of self-invertible matrix in stage one and stage two of hill cypher we can control the amount of encryption.

6. ACKNOWLEDGMENTS

The work described in this paper is supported by a grant from the *University Grants Commission,* New Delhi, India.

7. REFERENCES

[1] BibhudendraAcharya, GirijaSankarRath, Sarat Kumar Patra, Saroj Kumar Panigrahy. "Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm", *International Journal of Security*, Vol 1, Issue 1, pp. 14-21, 2007.

[2] BibhudendraAcharyaet. al, "Involutory, permuted and reiterative key matrix generation method for hill cipher system", International journal of recent trends in engineering, Vol. 1, No. 4, pp. 106-108, May 2009.

[3] BibhudendraAcharyaet. al, "Image encryption using Advanced hill cipher algorithm", International journal of recent trends in engineering, Vol. 1, No. 1, pp. 663-667, May 2009.

[4] Han Shuihunaet. al, "An asymmemtric Image Encryption Based on Matrix Transformation", ECTI Transaction on computer and information technology, Vol. 1, No. 2, pp 126-133, November 2005.

[5] H.S. kwok, Wallace k.S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation", Chaos, Solitons and Fractals 32 (2007) 1518-1529.

[6] Qu Wang , QingGuo , JinyunZhou , Double image encryption based on linear blend operation and random phase encoding in fractional Fourier domain, Optics Communications.

[7] Jun Li , Tao Zheng, Qing-zhi Liu, Rong Li, Double-image encryption on joint transform correlator using two-step-only quadrature phase-shifting digital holography, Optics Communications 285 (2012) 1704–1709.

[8] Panduranga H.T, Naveenkumar S.K, "A novel image encryption method using 4outof8 code", proc. CommV"09, pp 460 -462, 2009.

[9] GauravBhatnagar , Q.M. Jonathan Wu, Selective image encryption based on pixels of interest and singular value decomposition, Digital Signal Processing 22 (2012) 648–663.

[10] SapnaSasidharan and DeepuSleeba Philip, A Fast Partial Image Encryption Scheme With Wavelet Transform And

Rc4, International Journal of Advances in Engineering & Technology, Sept 2011.

[11] Xiongjun Li, A New Measure of Image Scrambling Degree Based on Grey Level Difference and Information Entropy, International Conference on Computational Intelligence and Security 2008.

[12] YueWu,Joseph P. Noonan and SosAgaian, NPCR and UACI Randomness Tests for Image Encryption, yber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011