SVITS-HDR a new Image Encryption Technique to encrypt high definition images

Nitin Rawal
Dept. of Information Technology
Shri Vaishnav Instt. Of Tech. and Sc. Indore

Manoj Dhawan
Astt. Prof. IT Dept.
Shri Vaishnav Instt. Of Tech and Sc. Indore

Abstract

In this paper, the author propose a method, SVITS-HDR, for image encryption, with high definition and resolution which basically has three stages: 1) in first stage image is divide into smaller chunks or shares, and these chunks and shares are shuffled within the image, each share of this image has a header value so we can regenerate this image at decryption. 2) In second stage, each pixel of image is converted to its equivalent 32 bit binary number and in that 32 bit number, the number of bits, which are equal to the length of password are rotated and then reversed, by extended bit rotation and reversal 3) In third stage, extended hill cipher technique is applied by using self invertible key matrix, to make it more secure. The technique presented in this paper is very good for encrypting any type of images, the first two stage of this image encryption is basically applied to reduce uniform background problem, and to secure from Known Plane Text attack. It can apply for high definition image up to 32 bit (8 bit each for RGB and 8 bit for alpha).

Keywords: **-** Image encryption, self invertible key matrix, bit rotation and reversal, hill cipher,

1. Introduction

Now days as multimedia data transfer over internet for communication is increased security of those data became an important issue in information security. Security of those data can be possible through different encryption algorithms, with the help of passwords. Many applications need multimedia encryption, such as pay-TV, e-commerce, sending private emails, transmitting financial information, security of ATM cards, multimedia data storage, and private medical information. Here we introduce a new image encryption algo for information security. This algo can use for very high definition and high resolution images. Reason to kept high definition is only to move more information securely over internet, like maps, telemedicine, multispectral image, military and other confidential services.

The rest of the paper is organized as follows: In Section 2 we surveyed image encryption algorithm which are previously proposed and also discussed problems with them. In section 3, proposal of new image encryption SVITS-HDR is located. In section 4, performance and comparison of encrypted image with plain image, conclusion is drawn in section 5.

2. Literature Survey

Komal D Patel and Sonal Belani [1] have presented a survey on existing work, which has used different techniques for image encryption as subject matter and also given a general introduction about cryptography. There are several methods for image encryption with some advantages and disadvantages. Ismet Ozturk and

Ibrahim Sogukpinaar [2] have discussed the analysis and comparison of image encryption algorithms. And they classified the image encryption methods into three major types: (i) position permutation, (ii) value transformation and (iii) visual transformation. Somdip Dey has proposed SD-AEI [3] Image encryption by bit modified rotation and reversal and Cyclic bit Rotation Followed by Extended hill cipher, with self invertible key matrix generation Key matrix [5]. This image encryption is successor of his previous technique SD-EI [6] with bit rotation and reversal with Advance hill cipher. This image encryption uses bit rotation and reversal for same no of bits, and for grey scale images. Bibhudendra Acharya et al [5] have proposed several methods of generating self-invertible matrix, which can be used in Extended Hill Cipher algorithm. Saroj Kumar Panigrahy et al [6] have implemented image encryption using Self-Invertible key matrix of Hill Cipher algorithm. Saroj Kumar Panigrahy et al [7] have proposed a novel Advanced Hill Cipher encryption technique, which uses Involutory key matrix. B.V. Rama Devi [8] propose a technique involves three stages. The first stage consists of encoding the image into a Gödel String. In the second stage the Gödel string is compressed using Alphabetic coding which in the third stage will be encrypted using a symmetric key cryptosystem or a public key cryptosystem.

These algorithms are good enough to encrypt low definition images and, mostly grey scale images, but as high definition images are in communication like military, telemedicine and other confidential services, to encrypt those images we have to apply any image encryption algo that is capable to encrypt image with high definition and high resolution like we propose below, SVITS-HDR.

3. Proposed Technique

We are presenting an image encryption method which comes in three stages which are described below,

3.1 Break image into smaller shares and shuffle within image: -

In this stage we break image into smaller chunk and those image chunks shuffle within this image, this permutation perform on the basis of random number generation, and each share of this image has its header value so that it can restore at the decryption phase. Here we consider an image with 6 vertical and 6 horizontal shares.

01	02	03	04	05	06
07	08	09	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36

Now we shuffle these share into the image, like e.g.

20	05	14	16	09	26
15	13	35	28	19	01
31	21	05	22	34	35
26	12	29	30	25	36
32	23	08	24	06	02
07	03	10	27	04	11

This shuffle is based on random number between 0 to (m*n) where m is the number of share in vertical direction and n is for horizontal direction.

3.2 Advance Bit Rotation and Reversal

A bit rotation and reversal is proposed by Somedip dey [4], here we made an advance step in this by calculating a password length in other way, we are taking the image pixel length up to 32 bits and a password is given along with the plain image. Now effective length of password is considered for bit rotation and reversal. i.e., Number of bits to be rotated to left and reversed will be decided by the sum of ASCII value of each character of password mod by total number of bits. Let L be the length of the password and N be the number of bits to be rotated to left and reversed (i.e. N is the effective length of password).

The relation between L and N is represented by equation (1).

N = [C0+C1+C2+………+Cn] mod 32

------ eq. (1)

Where C is the character of password at nth position and n=0, 1, 2, 3, 4,....L. now each value of a pixel is converted into 32 bit binary number, this binary number passes through bit rotation and reversal technique.

Let P (I, J) is a decimal value of a pixel being converted into decimal number is

[**b**0,**b**1,**b**2,**b**3,**b**4,**b**5,**b**6,**b**7,**b**8,**b**9,**b**10,**b**11,**b**12,**b**13,**b**14,**b**15,**b**16,**b**17,**b**18,**b**19,**b**20,**b**21,**b**21,**b**23,**b**24,**b**25,**b**26,**b**27,**b**28,**b**29,**b**30,**b**31,**b**32]

Now suppose that password is AaBbCc then the password length is 6 and the effective length is

[65+97+66+98+67+99] mod 32=12

So 12 bits have to get rotate towards left, so the pixel value will became

[**b**13,**b**14,**b**15,**b**16,**b**17,**b**18,**b**19,**b**20,**b**21,**b**21,**b**23,**b**24,**b**25,**b**26,**b**27,**b**28,**b**29,**b**30,**b**31,**b**32,**b**0,**b**1,**b**2,**b**3,**b**4,**b**5,**b**6,**b**7,**b**8,**b**9,**b**10,**b**11,**b**12]

And get reversed as

[**b**13,**b**14,**b**15,**b**16,**b**17,**b**18,**b**19,**b**20,**b**21,**b**21,**b**23,**b**24,**b**25,**b**26,**b**27,**b**28,**b**29,**b**30,**b**31,**b**32,**b**12,**b**11,**b**10,**b**9,**b**8,**b**7,**b**6,**b**5,**b**4,**b**3,**b**2,**b**1,**b**0]

We apply this process for each pixel of shuffled image after first step

3.3 Use of Hill cipher

In this stage we apply hill cipher to encrypt this permutated image generated in step 2. As we know that inverse of a key matrix is needed to decrypt image so we use self invertible key matrix [5] to get key matrix and use this key matrix in hill cipher to get final encrypted image.

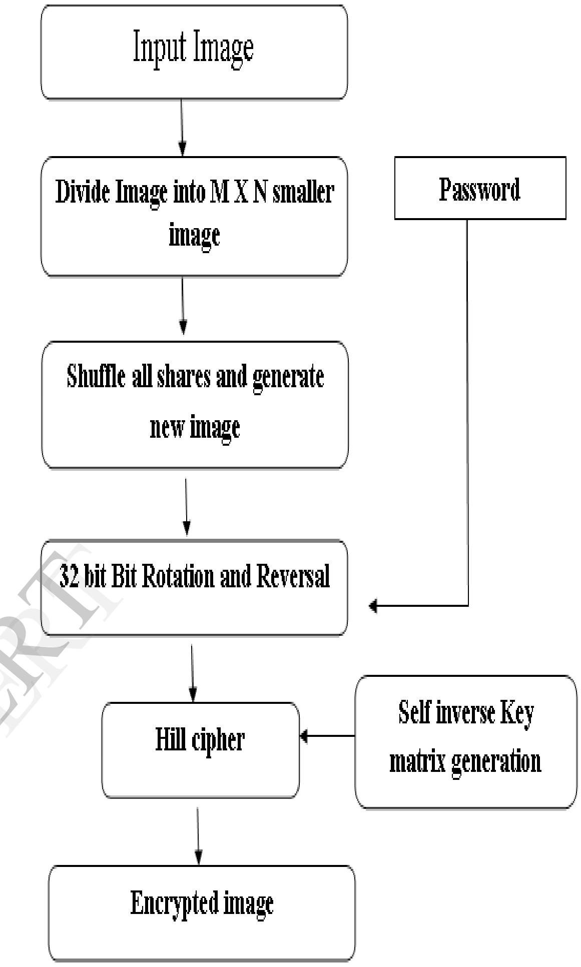
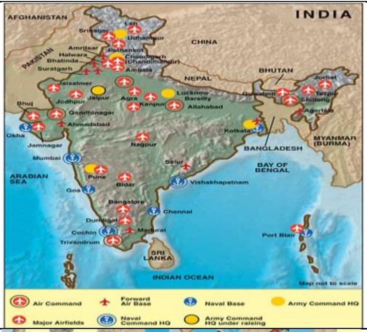

Input Image
Divide Image into M X N smaller image
Password
Shuffle all shares and generate new image
32 bit Bit Rotation and Reversal
Hill cipher
Self inverse Key matrix generation
Encrypted image

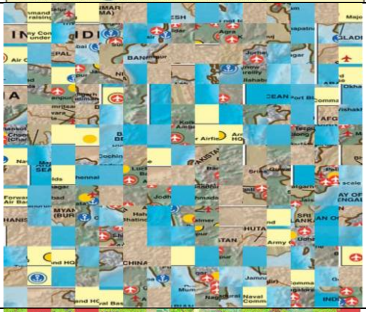
Fig.1. Architecture of Proposed scheme SVITS-HDR

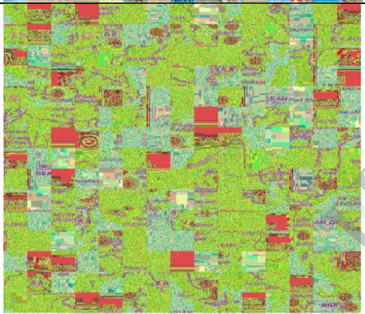
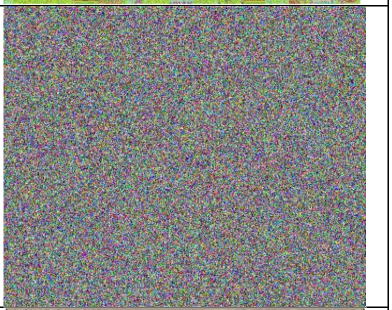
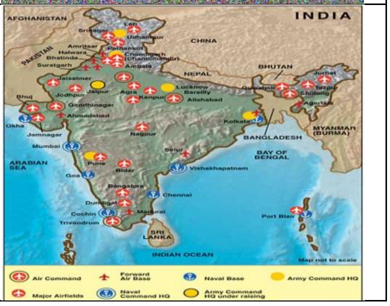
4. Experiment Results

In table 1 we include experimental result by this image encryption algorithm. In first row there is an image for input, in second we have break image into smaller chunks and permuted them into the image to create a new image. The next row shows Advance bit rotation and reversal, made binary rotation with pixel values.

Table 1.0 Shows result of SVITS-HDR stages.

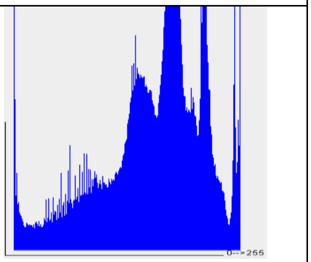
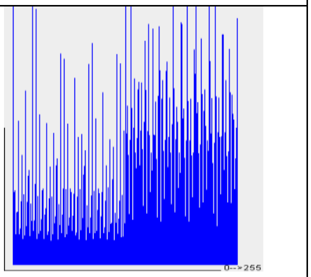
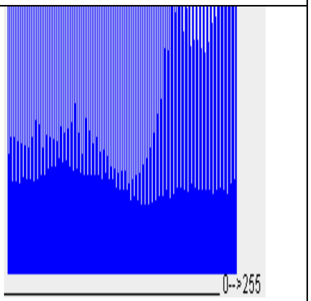
Stage	Image
Plane	 INDIA AFGHANISTAN PAKISTAN CHINA NEPAL BHUTAN BANGLADESH MYANMAR (BURMA) ARABIAN SEA BAY OF BENGAL SRI LANKA INDIAN OCEAN Map not to scale Air Command Forward Air Base Naval Base Army Command HQ Major Airfields Naval Command HQ Army Command HQ under raising

Shuffled
V=15
H=15
	

Password = Nibtahi Advanced Bit Rotation and reverse	
Hill cipher	
Decrypted	 INDIA AFGHANISTAN PAKISTAN CHINA NEPAL BHUTAN BANGLADESH MYANMAR (BURMA) ARABIAN SEA BAY OF BENGAL SRI LANKA INDIAN OCEAN Map not to scale Air Command Forward Air Base Naval Base Army Command HQ Major Airfields Naval Command HQ Army Command HQ under raising

We apply this image encryption algo on a high definition 32 bit image (8 bit for RGB each and 8 bit for Alpha) with 4320 into 3240 resolution; found no loss of pixel data in this process.

Table 2. Some Experiment results of SVITS-HDR.

Stage	Histogram
Plane	
Advanced Bit Rotation and reverse	 RED:- Dark blue, Green:- Normal Blue Blue:- Light Blue
Hill cipher	
Difference between Decrypted and Plain image	

5. Conclusion and future scope

As we know that hill is less secure for known plain text attack so we have decided to use first two stages as in support to this cipher so that we can overcome uniform background problem. Proposed scheme is simple and an easy way to encrypt images. At decryption side we can use the password and key matrix to decrypt images. This scheme can be used in future to encrypt image and into a combination of a steganography and image encryption scheme, where message is already hidden into an image. It can be widely applied in other information security fields such as video encryption.

References

[1]. Nitin Rawal, Manoj Dhawan "*A Survey Report on Image encryption techniques*" International Journal of Engineering Research and Technology. Vol. 2 (10), 2013, ISSN 2278 – 0181. October 2013

[2]. Komal D Patel, Sonal Belani, "*Image encryption using different techniques:A review*", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 1, November 2011

[3]. Ismet Ozturk and Ibrahim Sogukpinaar, "*Analysis and Comparison of Image Encryption Algorithms*", Transaction on engineering, Computer and Technology, 2004, vol.3, pp.38-42.

[4]. Somdip Dey, "*Amalgamation of Cyclic Bit Operation in SD-EI Image Encryption Method: An Advanced Version of SD-EI Method: SD-EI Ver-2*", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3): 221-225 The Society of Digital Information and Wireless Communications (SDIWC) Nov. 2012 (ISSN: 2305-0012).

[5]. Somdip Dey, "*SD-EI: A Cryptographic Technique To Encrypt Images*", Proceedings of "The International Conference on
Cyber Security, CyberWarfare and Digital Forensic (CyberSec 2012)", held at Kuala Lumpur, Malaysia, 2012, pp. 28-32.

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

[7]. Saroj Kumar Panigrahy, Bibhudendra Acharya, Debasish Jena, "*Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm*", 1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.

[8] Saroj Kumar Panigrahy, Bibhudendra Acharya, Debasish Jena, "*Image Encryption Using Self-Invertible Key Matrix of HillCipher Algorithm*", 1st International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.

[9]. Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "*Image Encryption Using Advanced Hill Cipher Algorithm*", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009, pp. 663-667.

[10] B.V.Rama Devi B.V. Rama Devi, "*A New Encryption Method for Secure Transmission of Images*" (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 2801-2804

[11].http://en.wikipedia.org/wiki/RSA_(algorithm) [ONLINE]

[12]. http://en.wikipedia.org/wiki/Elliptic_curve_cryptography [ONLINE]

[13]. Cryptography & Network Security, Behrouz A. Forouzan, Tata McGraw Hill Book Company.