Modified Key Based Image Encryption using RSA algorithm

Devashish Vaghela[1], Prof. RajyaLakshmi Jaiswal[2]
[1]*P.G. Student, Computer Engineering, L.D. Engineering college, Ahmadabad, Gujarat, India*
[2]*Asst. Professor, L.D. Engineering college, Ahmadabad, Gujarat, India*

Abstract- **Security of data is major point of concern in our day to day transfer of information. Data could be anything image data, stream data so in order to improvise security of data we have studied different type of cryptography algorithm here our major area of data is image security because now a days image transfer is more confidential thing which includes medical imaging, space analysis images. We have studied different type of encryption technique like bit rotation, bit reversal, matrix multiplication. Here during our literature study we found existing encryption techniques uses secret key in order to encrypt and decrypt image so here we can increase security of image sharing using public private key pair.**

Index Terms**—** **Image Encryption, Hill Cipher, Bit rotation, Bit reversal**

I. INTRODUCTION

Now a day's world is going towards digital media.

So in general thinking it is good there will be less human efforts and more time and work potential utilization but digitalization comes with big security and vulnerability threats. In present scenario we transfers many confidential image files through digital gadgets.

There can be possibility that our data will be intercepted by any unwanted personal to whom we don't want to share our valuable data. So to avoid such circumstance encryption of image file is required and basically security of data is main point of concern.

Image data security can be ensured by applying encryption to the images or by using various types of image watermarking techniques.

- Digital pictures are generally bigger in size than that of plain content. Along these lines, the routine framework sets aside more opportunity for scrambling the advanced picture information.
- Original and decoded content ought to be same. Yet, this prerequisite is a bit much for picture information.

There are many ways for image encryption like position permutation, value transformation, and visual transformation etc. In permutation, transformation and randomization we use random bit manipulation on image pixels.

Image transformation and visual transformation involves manipulation data, it can be a single image or two or more images of the same area acquired at different times.

Image transformation generates "new" images from two or more sources which highlight features or properties of interest like edges, details of pixels, intensity measures.

II. BACK GROUND

The image encryption is process to transmit image securely over network so we can make sure that only intended user can decrypt image. Video encryption, image encryption, chaos based encryption have applications in many fields including medical imaging, Tele-medicine, military Communication, etc. The evolution of encryption is moving towards a future of endless possibilities.

Due to vast sources of digital techniques for transmitting and storing images are available, it becomes an important point of concern that how to protect the confidentiality, integrity and authenticity of images which requires to transmit among several nodes. The image data have properties like bulk capability, high redundancy, and high correlation among the pixels. Image can be of different types like grey scales images, image having similar background. Image encryption techniques scrambles the pixels of the image and decrease the correlation among the pixels, so correlation deference as well as change of frequency among pixels will be changed and we will obtain encrypted image data. In next article I have discussed different type of security analysis concepts like histogram, entropy, correlation, key space.

III. PROPOSED APPROACH

In our proposed approach during Image encryption we uses alphanumeric secret password key instead of it we can derive a key pair from key generator designed from RSA algorithm. Using key pair derived from RSA we can protect secret key that we uses in Image encryption process so there will be two level security of secret key will be there. In RSA we can increase domain for prime no choice to resist against brute force attack and we can also increase key size in order to improve security. Here using combination of symmetric and asymmetric approach I have tried to resolved key management issue of image encryption.

Key Generation:

Using RSA algorithm we selects two large set of prime integer no's and using those two no's we encrypt our secret key.

Secret key of image will be alpha numeric value of 8 letters and after that we selects ASCII value of each letter of alpha numeric password and after that we multiplies it to position of letter in word and after computing this values for all letters at the end we will sum up all values of each letter and at the end we gets code of alpha numeric code. This key we protects with RSA key pair so two factor security of key will be provided and issue of secret key security can be resolved as whom we intends can only decrypt key as other node won't have private key available to decrypt secret key.

Bit Rotation technique:

In bit rotation technique we will first converts image provided into grey scale images so image will be converted from color image to grey scale images after that we create matrix representation of image programmatically and each pixel of image will have 8 bits as image having intensity from 0 to 255 so each pixel represents 8 bits.Now we have code value of secret key which we have encrypted during image sharing, following formulae will be apply to that code value.

Shifts = Code mod 7

Here we used mod 7 because mod 7 will reverse entirely pixel of image. The resultant value we get from shift operation will be value of bit shift that will be applied to each pixel of image. Now shift we get from above formulae times bit will be shifted to left and this technique applies to whole image. So partial encryption of image is done.

Image block creation:

During image block creation we creates 3*3 blocks of image using size and resolution of image and blocking process of image can be done programmatically.

Modified Hill Cipher Technique:

Now we have partially encrypted set of image blocks available. We will pass this partial encrypted image to our modified hill cipher technique. We can apply hill cipher only if matrix we uses have inverse of matrix should be available so here we can further optimized our time using involutory matrix i.e matrix that is own inverse of itself.

We multiplies each block of image to involutory matrix so now each pixel values are shuffled so it will be difficult for interceptor to analyze image properly. Block creation of image shuffles entire partial encrypted image and further use of matrix multiplication using modified hill cipher technique further optimizes encryption process.

Bit Reversal Technique:

In bit reversal technique we takes partial encrypted image from hill cipher and pass it to bit reversal process. In this technique next level of bit level shuffling is done and entire set of bits of pixel gets reversed so each pixels consist 8 bits and this 8 bits values will be shuffled entirely this ends our encryption process of image.

Encryption:

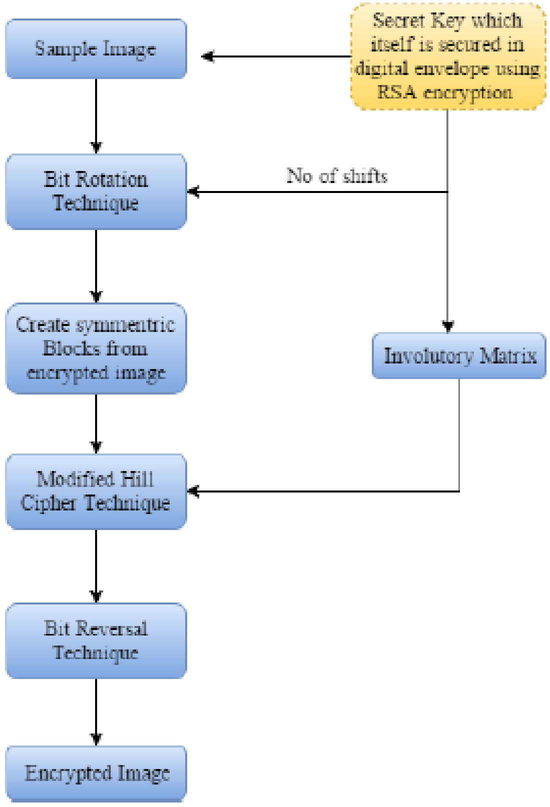

Sample Image
Secret Key which itself is secured in digital envelope using RSA encryption
Bit Rotation Technique
No of shifts
Create symmentric Blocks from encrypted image
Involutory Matrix
Modified Hill Cipher Technique
Bit Reversal Technique
Encrypted Image

Figure 1: Proposed encryption approach

Decryption:

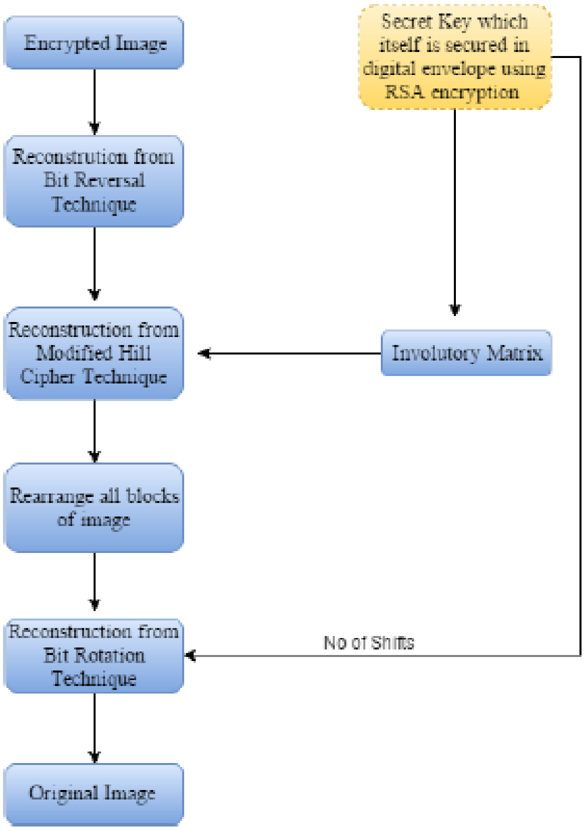
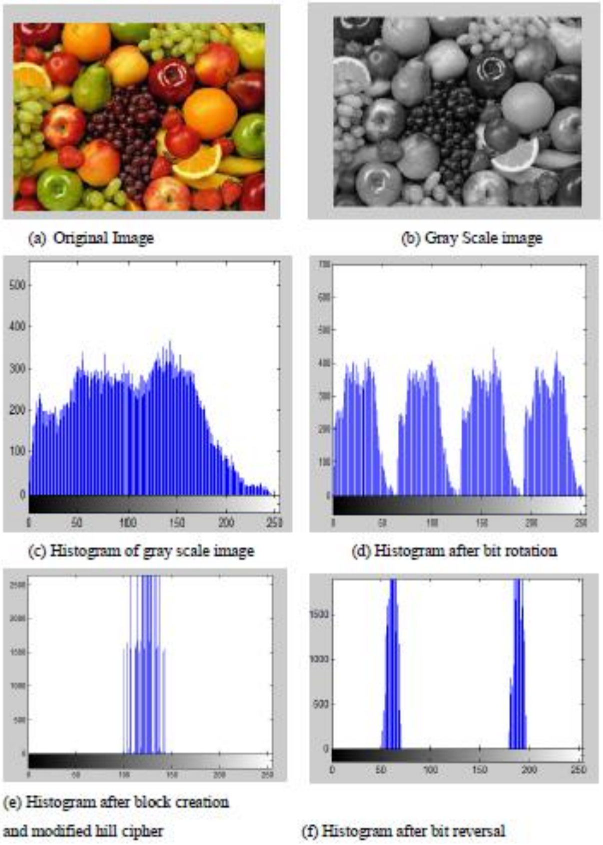

Encrypted Image
Secret Key which itself is secured in digital envelope using RSA encryption
Reconstrution from Bit Reversal Technique
Reconstruction from Modified Hill Cipher Technique
Involutory Matrix
Rearrange all blocks of image
Reconstruction from Bit Rotation Technique
No of Shifts
Original Image

Figure 2: Proposed Decryption approach

Analysis of Proposed Image Encryption Technique.

Following diagram shows example of histogram generated after sample image encrypted by proposed technique. From histogram we can see that we are getting uniform distributed pixels values after each level of encryption process. So our encryption technique gives expected better results.



(a) Original Image

(b) Gray Scale image

(c) Histogram of gray scale image

(d) Histogram after bit rotation

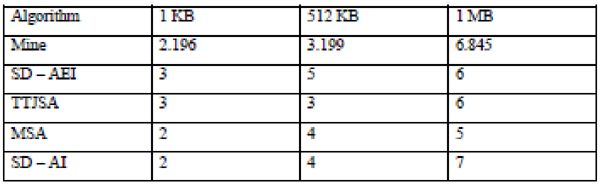
(e) Histogram after block creation and modified hill cipher

(f) Histogram after bit reversal

Figure 3: Histogram analysis

Time Analysis

Following table gives idea about amount of time required to encrypt and decrypt image using our encryption algorithm compare to others from this table we can see that our encryption technique take less time for small as well as large grey scale images



Algorithm	1 KB	512 KB	1 MB
Mine	2.196	3.199	6.845
SD – AEI	3	5	6
TTJSA	3	3	6
MSA	2	4	5
SD – AI	2	4	7

Table 1: Time comparision with other algorithm

IV. CONCLUSION

Based on study of image encryption techniques we found that using bit rotation, reversal, mathematical models and matrix manipulation techniques we can encrypt images. This techniques can be very useful in medical imaging, space applications, and social media application. In existing methods we found there can be vulnerable attacks on password secret key that we are using for bit rotation and reversal, extended hill cipher. In order to improve security of image data encryption we proposed algorithm that uses password generated using RSA algorithm. So due to this modification security of password key will be increased to brute force attack. We measured performance using parameters Histogram, time analysis.

REFERENCES

[1] http://www.garykessler.net/library/crypto.html

[2] http://searchsecurity.techtarget.com/definition/RSA

[3] http://searchsoftwarequality.techtarget.com/definition/cryptography

[4] https://www.cs.utexas.edu/~mitra/honors/soln.html

[5] B Acharya, S Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "*Image Encryption Using Advanced Hill Cipher Algorithm*", ACEEE, Vol 1, No. 1, Jan 2010

[6] Somdip Dey, Sriram S. Ayyar, S.B. Subin, P .K. Abdul Asis,"*SD-IES: An Advanced Image Encryption tandard Application of Different Cryptographic Modules in a New Image Encryption System*",IEEE,2012

[7] Asoke Nath, Saima Ghosh, Meheboob Alam Mallik,"*Symmetric Key Cryptography using Random Key generator*", "Proceedings of International conference on security and management (SAM'10" held at Las Vegas, USA Jull 12-15, 2010), P-Vol-2, pp. 239-244 (2010).

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

[9] S 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,IEEE,2012.

[10] Asoke Nath, Trisha Chatterjee, Tamodeep Das, Joyshree Nath, Shayan Dey, "*Symmetric key cryptosystem using combined cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm*", Proceedings of "WICT, 2011 " held at Mumbai, 11th – 14th Dec, 2011, Pages:1175-1180.

[11] S Dey, "*SD-AEI: An advanced encryption technique for images*", 2012 IEEE Second International Conference on Digital Information Processing and Communications
(lCDIPC), pp. 69-74.

[12] S Dey, "*An Image Encryption Method: SD-Advanced Image Encryption Standard: SD-AIES*", (IJCSDF) 1(2): 82-88, (ISSN: 2305-0012)

[13] Rajput Y, Gulve A, "*An Improved Cryptographic Technique to Encrypt Images using Extended Hill Cipher*", International Journal of Computer Applications (0975 – 8887) Volume 83 – No 13, December 2013.

[14] Sami A. Nagar and Dr. Saad Alshamma,"*Efficient Implementation of RSA Algorithm with MKE"* ,IEEE 2012

[14] Ghosh C, Mandal S,"*A Combined Method for Image Encryption*", IJERA, ISSN: 2248-9622 National Conference on Advances in Engineering and Technology (AET- 29th March 2014)

[15] S. Emalda Roslin, N.M. Nandhitha, Anita Daniel, "*Transposition Based Symmetric Encryption and Decryption Technique for Secured Image Transmission through Internet*",
IEEE,2014 [16] Binay singh,Sudhir Kumar Gupta,*"Grid-based Image Encryption using RSA"*,IJCA,april-2015

[17] Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran,*"Digital Image Encryption Based on RSA Algorithm",IOSR-JECE Jan 2014*

[18] Rinaldi Munir,*"Security Analysis of Selective Image Encryption Algorithm Based on Chaos and CBC-like Mode"*, IEEE 2012