International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 12th Dec 2022. Link :http://www.ijiemr.org/downloads.php?vol=Volume-11&issue=Issue 12

DOI: 10.48047/IJIEMR/V11/ISSUE 12/67

Title **A NEW LOSSLESS IMAGE CRYPTOSYSTEM OF COLOR IMAGES FOR SECURITY APPLICATIONS**

Volume 11, ISSUE 12, Pages: 536-545

Paper Authors
K. Shirisha, V Supriya Reddy, B Umaparvathi, Parsha Deekshith, Ramagiri Raviteja

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A NEW LOSSLESS IMAGE CRYPTOSYSTEM OF COLOR IMAGES FOR SECURITY APPLICATIONS

K. Shirisha[1], V Supriya Reddy[2], B Umaparvathi[2], Parsha Deekshith[2], Ramagiri Raviteja[2]

[1]Assistant Professor, [2]UG Scholar, [1,2]Department of Electronics and Communication

[1,2]Malla Reddy Engineering College and Management Sciences, Medchal, Telangana.

ABSTRACT

In Recent years digital image security plays an important role in communication and even in many applications such as military, medical, civil applications. Secured digital image will be very use full for storage and transmission applications. Hence, it becomes an important and challenging task for organizations, industries, individuals and even for governments as well. Cryptanalysis or cryptosystem is an effectual technique to secure digital images or videos by translating them into an ungrasped manner. There are so many approaches have been developed for image cryptanalysis. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are the possible cryptosystems, which considers input image as data blocks or streams. However, DES and AES methods produce large computational costs and poor error resilience. To reduce the computational time and even cost researchers have introduced a new approach for image cryptosystem which is based on the combination of image bit plane decomposition and arithmetic logic operations. Even though the security level of this method is much lower because the results of its decomposition process and logic operations are predictable. To achieve higher levels of security, one solution is to change image pixel values while scrambling the positions of image pixels or blocks using different techniques.

Keywords: Cryptosystem, lossless encryption, security applications.

1. INTRODUCTION

Network technologies and media services provide ubiquitous conveniences for individuals and organizations to collect, share, or distribute images/videos in multimedia networks and wireless or mobile public channels. Image security is a major challenge in storage and transmission applications. For example, video surveillance systems for homeland security purposes are used to monitor many strategic places such as public transportation, commercial and financial centers. Large amounts of videos and images with private information are generated, transmitted, or restored every day. In addition, medical images with a patient's records may be shared among the doctors in different branches of a health service organization over networks for different clinical purposes. These images and videos may contain private information. Providing security for these images and videos becomes an important issue for individuals, business, and governments as well. Moreover, applications in the automobile, medical, construction and fashion industry require designs, scanned data, and blueprints to be protected against espionage. Considering the long lifetime of image in the afore-mentioned domains, it is imperative to develop and employ techniques which protect the content throughout their lifetime. Image encryption is an effective approach to protect images or videos by transforming them into completely different formats Several interesting approaches for image encryption have been developed. One method based on the cryptography concept considers images as data blocks or streams. It encrypts images block by block or stream by stream using different techniques. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are two examples of this approach. However, such encryption methods incur large computational costs and show poor error resilience.

Image encryption can be accomplished by scrambling image pixel positions using different techniques in the spatial domain. One example is the recursive sequence-based image scrambling approach. It scrambles images using different recursive sequences such as the Fibonacci sequence, Cellular automata, and chaotic maps. Image encryption can also be accomplished by scrambling coefficient matrices/blocks in the transform domain. Nevertheless, these approaches have extremely low security levels due to the lack of security keys or the small key space. Furthermore, the permutation-only based encryption schemes are known to be vulnerable for plaintext attacks. Another approach for image encryption is to change image pixel values based on the combination of image bit plane decomposition and logic operations. The security level of this method is much lower because the results of its decomposition process and logic operations are predictable. It is not immune to plaintext attacks.

To achieve higher levels of security, one solution is to change image pixel values while scrambling the positions of image pixels or blocks using different techniques. In this paper, we introduced a new gray/RGB image encryption and decryption algorithm using edge mapped combined key generation (EM-CKG), which is a binary image with the same size as the original image to be encrypted.

Steganography is one of the data hiding technique in which Secret communications take place that conceal the very existence of the message. Cryptography in another type of data hiding technique in which message to be hidden is encoded using encryption or coding techniques. Here we know that a message is there but cannot understand it. Watermarking is another technique in which information that is hided is directly related to the item in which it is embedded.

On the other hand, in visual cryptography or visual secret sharing (vss), the original input image is shared between a set of participants P by a dealer (secret image holder). Based on the sharing policy, only qualified subsets of participants can recover the original input image.

Two important factor s that used to determine the efficiency of any visual cryptography scheme, namely:

1) The quality of the reconstructed image and
2) The pixel expansion (m).

Any loss of information during the reconstruction phase leads to reduction in the quality of the recovered image. On the other hand, pixel expansion refers to the number of sub pixels in the generated shares that represents a pixel of the original input image. For bandwidth constrained communication channels, it is desirable to keep m as small as possible. For color images, reducing pixel expansion is of paramount importance since they occupy more space and consume more bandwidth compared to grayscale and binary images. Most of the previous works in this area try to optimize pixel expansion or obtain perfect reconstruction.

In Visual Cryptography schemes (VCS) the traditional stacking operation of sub pixels and rows interrelations is modified. This new technique does not require transparencies stacking and hence, it is more convenient to use in real applications. However, it requires the use and storage of a Color Index Table (CIT) to losselessly recover the secret image. CIT requires space for storage and time to look up the table. Also, if number of colors c increases in the secret image, CIT becomes bigger, and the pixel expansion factor becomes significant which results in severe loss of resolution in the camouflage images. Ours is an advanced scheme for hiding a colored image into multiple images that does not require a CIT. This technique achieves a lossless recovery of the secret image, but the generated shares (camouflage images) contain excessive noise.

Visual cryptography is a new cryptographic scheme where the cipher text is decoded by the human visual system. Hence, there is no need to any complex cryptographic computation for decryption. The idea is to hide a secret message (text, handwriting, picture, etc…) in different images called shares or cover images. When the shares (transparencies) are stacked together to align the sub pixels, the secret message can be recovered. The simplest case is the 2 out of 2 schemes where the secret message is hidden in 2 shares, both needed for a successful decryption. This can be further extended to the k out of n scheme where a secret message is encrypted into n shares but only k shares are needed for decryption where k≤ n. If k-1 shares are presented, this will give no information about the secret message. The inconvenience with the previous schemes was that they used meaningless shares to hide the secret and the quality of the recovered plain text is bad. More advanced schemes based on visual cryptography where a colored image is hidden into multiple meaningful cover images is a new colored secret sharing and hiding scheme.

2. LITERATURE SURVEY

From the previous decades there are such a large number of picture cryptographic algorithms have been created to shield the pictures from unauthorized gatherings, which were hoping to pulverize the information sent by transmitter. In 1995 the principal picture and video encryption: from digital rights administration to secured personal communication distributed by Pommer Andreas and Uhl Andreas. In [1] the creators said that an incorporated outline of plans for encryption of pictures and videos will be given by picture and video encryption. This reaches from couple of business applications like digital video broadcasting (DVB) or digital audio broadcasting (DAB) to more research situated points and distributed substance. The idea in [2] was distributed by B. Schineir, in which the theorital and viable learning of a cryptosystem has been given to secure the multimedia. It was presented in 1995 and soon it turned into the standard reading material for cryptography courses in everywhere throughout the world. The creator in [3] proposed another invertible 2D map, called Line map, for encryption and decoding of picture, which maps a picture into a variety of pixels and after that maps it back to the first picture. This methodology demonstrates the preferred execution over the beforehand existed 2D maps, in which just change was utilized. Another methodology for picture encryption in [4], which is proposed by kuang tsan lin, this methodology used the both enchantment network scrambling and binary coding technique to shape a half breed encoding strategy to scramble a picture. This won't give any kind of contortion in decoding process, which means that the precise unique picture will be recuperated at the collector end. Anil kumar et. al. in [5] presented another picture encryption technique in light of disordered standard guide which utilizes expanded substitution-dispersion plan. This strategy utilizes straight input shift register to conquer the downsides of existing techniques by including nonlinearity. This methodology is very secured and speedier than the customary strategies. Zhi liang zhu et. al. [6] presented a tumult based symmetric picture encryption utilizing a bit level change, in which the Arnold feline guide for bit level stage proposed for a picture cryptosystem to give more security and speedier reproductions. A successful, secured, quick and savvy picture transmission plan proposed in [7] utilizes encryption, compression and secured key trading alongside the picture transmission. As of late, a picture encryption plan considering partial Fourier transform (FRFT), solitary worth disintegration and Arnold transform has been proposed in [10] to enhance the security to improve the nature of decrypted picture. Picture encryption technique utilizing bit plane deterioration and scrambling was proposed by qiudong sun [8], which goes for the pixels positions exchanging and changing the dim estimations of pixels in the meantime. This methodology has preferable proficiency and properties over the arbitrary scrambling techniques and it has more stability degree than the traditional strategies, for example, Arnold transform.

PREVIOUS ENCRYPTION TECHNIQUES

2.1 The Data Encryption Standard (DES)

As mentioned earlier there are two main types of cryptography in using today - **symmetric** or **secret key** cryptography and **asymmetric** or **public key** cryptography. Symmetric key cryptography is the oldest type whereas asymmetric cryptography is only being used publicly since the late 1970's[1]. Asymmetric cryptography was a major milestone in the search for a perfect encryption scheme. Secret key cryptography goes back to at least Egyptian times and is of concern here. It involves the use of only one key which is used for both encryption and decryption (hence the use of the term symmetric).

To accomplish encryption, most secret key algorithms use two main techniques known as **substitution** and **permutation**. Substitution is simply a mapping of one value to another whereas permutation is a reordering of the bit positions for each of the inputs. These techniques are used a few times in iterations called **rounds**. Generally, the more rounds there are, the more secure the algorithm. A non-linearity is also introduced into the encryption so that decryption will be computationally infeasible[2] without the secret key. This is achieved with the use of S-boxes which are basically non-linear substitution tables where either the output is smaller than the input or vice versa.

1) It is claimed by some that government agencies knew about asymmetric cryptography before this.
2) This means that it costs more to implement the attack than the information is worth.

One of the main problems with secret key cryptography is **key distribution**. For this form of cryptography to work, both parties must have a copy of the secret key. This would have to be communicated over some secure channel which, unfortunately, is not that easy to achieve. As will be seen later, puplic key cryptography provides a solution to this.

3. PROPOSED IMPLEMENTATION

Here, we are going to implement the new image encryption and decryption algorithm in such a way that it allows to encrypt and decrypt both 3D images i.e., Key image and original image and more importantly, we had implemented new combined key generation (CKG) scheme that uses two key images for improving the security.

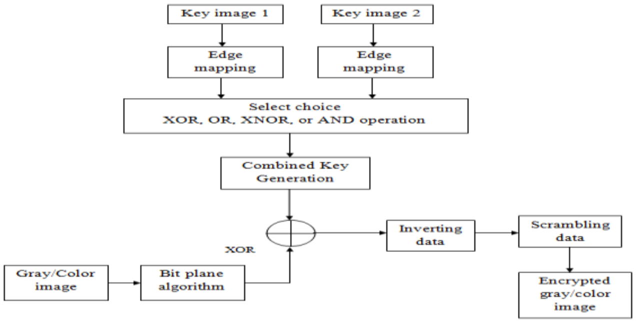


Fig. 1: Block diagram of proposed EM-CKG encryption.

Encryption Algorithm

Step 1: Select and read a gray/color (RGB) image to be encrypted

Step 2: Now, convert the image into number of bit planes using bit plane algorithm i.e., for gray scale '8' bit planes and for RGB image '24' bit planes

Step 3: Now select and read the two key images with the same size of input image.

Step 4: Apply edge mapping to get the binary information

Step 5: Now, apply combined key generation to the new key image by considering XOR, AND, XNOR, and OR operations for the encryption based on user's choice.

Step 6: Then do the XOR of bit planes of original gray/RGB image with the new key image.

Step 7: Then the XORed image will be inverted i.e., the bit planes of image will be shuffled for improving the security.

Step 8: Then we had done scrambling operation for more security concern using number to string and binary to decimal operations.

Step 9: Finally, we had a fully encrypted image with the CKG algorithm.

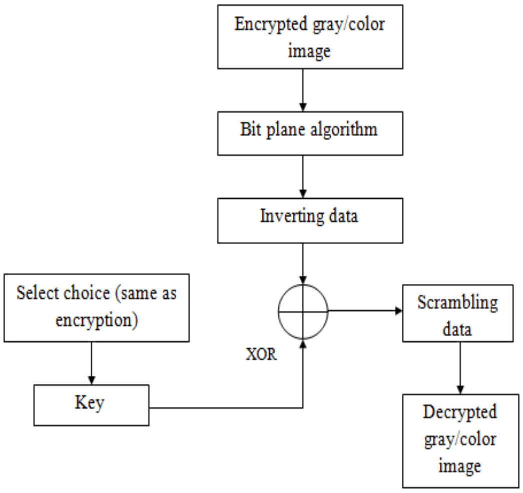
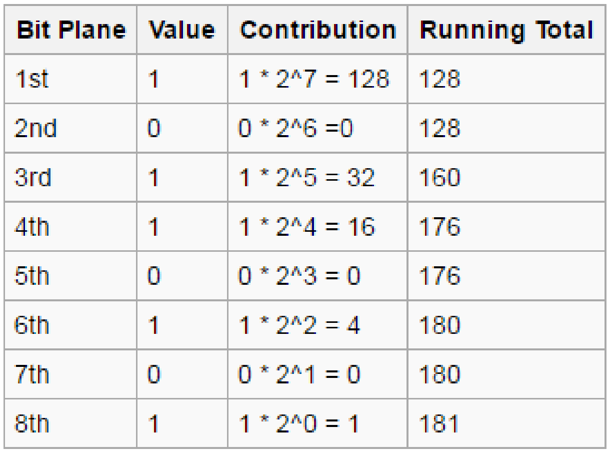

Encrypted gray/color image
Bit plane algorithm
Inverting data
Select choice (same as encryption)
XOR
Scrambling data
Key
Decrypted gray/color image

Fig. 2: Proposed decryption algorithm.

Bitplane Algorithm

A bit plane of a digital discrete signal (such as image or sound) is a set of bits corresponding to a given bit position in each of the binary numbers representing the signal. For example, for 16-bit data representation there are 16 bit planes: the first bit plane contains the set of the most significant bit, and the 16th contains the least significant bit. It is possible to see that the first bit plane gives the roughest but the most critical approximation of values of a medium, and the higher the number of the bit plane, the less is its contribution to the final stage. Thus, adding a bit plane gives a better approximation. If a bit on the nth bit plane on an m-bit dataset is set to 1, it contributes a value of $2^{(m-n)}$, otherwise it contributes nothing. Therefore, bit planes can contribute half of the value of the previous bit plane.

For example, in the 8-bit value 10110101 (181 in decimal) the bit planes work as follows:



Bit Plane	Value	Contribution	Running Total
1st	1	1 * 2^7 = 128	128
2nd	0	0 * 2^6 =0	128
3rd	1	1 * 2^5 = 32	160
4th	1	1 * 2^4 = 16	176
5th	0	0 * 2^3 = 0	176
6th	1	1 * 2^2 = 4	180
7th	0	0 * 2^1 = 0	180
8th	1	1 * 2^0 = 1	181

Bitplane is sometimes used as synonymous to Bitmap; however, technically the former refers to the location of the data in memory and the latter to the data itself. One aspect of using bit-planes is determining whether a bit-plane is random noise or contains significant information. One method for calculating this is compare each pixel (X,Y) to three adjacent pixels (X-1,Y), (X,Y-1) and (X-1,Y-1). If the pixel is the same as at least two of the three adjacent pixels, it is not noise. A noisy bit-plane will have 49% to 51% pixels that are noise.

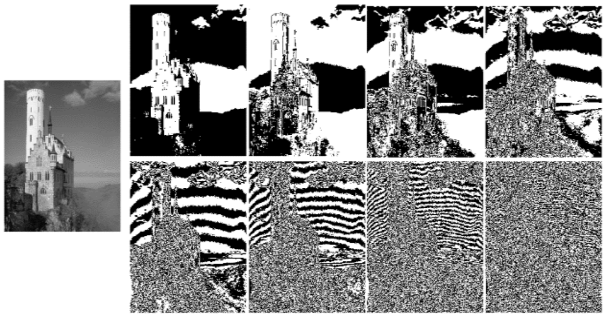


Fig. 3: Example of a gray scale image bit planes.

Inverting

Inversion is done by using a command *"fliplr",* which is used to flip an array form left to right. This process is used to provide more secure concern to encrypted image after applying logical operations.

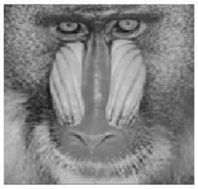
Scrambling Algorithm

Here, the scrambling is done by using number to string and binary to decimal operations

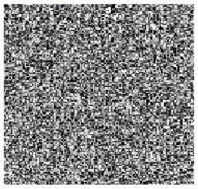
4. EXPERIMENTAL RESULTS

ORIGINAL IMAGE

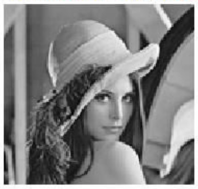
KEY IMAGE



ENCRYPTED IMAGE OF GRAY SCALE IMAGE



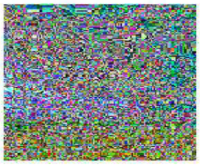
DECRYPTED GRAY SCALE IMAG



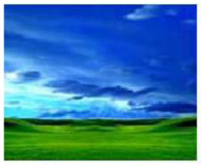
ORIGINAL IMAGE

KEY IMAGE

ENCRYPTED IMAGE OF COLOUR IMAGE



DECRYPTED COLOUR IMAGE

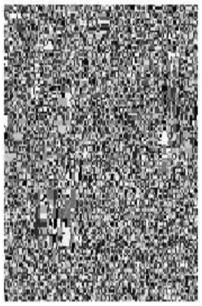


International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

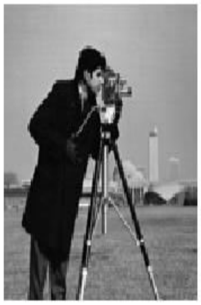
ORIGINAL IMAGE

KEY IMAGE

ENCRYPTED IMAGE OF GRAY SCALE IMAGE



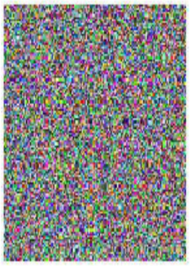
DECRYPTED GRAY SCALE IMAGE



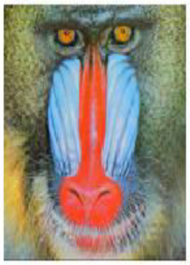
ORIGINAL IMAGE

KEY IMAGE

ENCRYPTED IMAGE OF COLOUR IMAGE



DECRYPTED COLOUR IMAGE

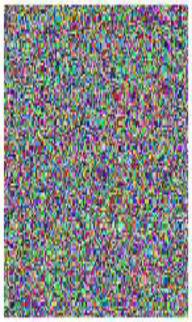


ORIGINAL IMAGE

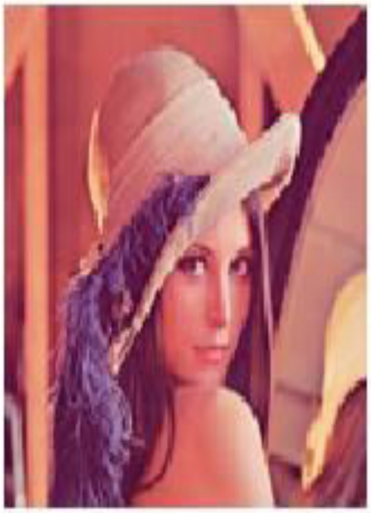
KEY IMAGE-1

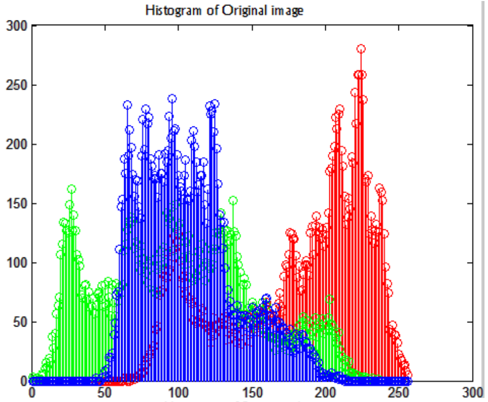
KEY IMAGE-2

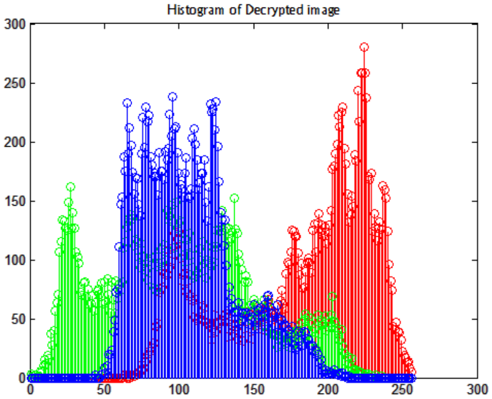
ENCRYPTED IMAGE OF COLOUR IMAGE



DECRYPTED COLOUR IMAGE







5. CONCLUSION

In this article, we introduced a new gray/RGB image encryption and decryption algorithm using edge mapped combined key generation (EM-CKG) with logical operations and scrambling approaches. The proposed algorithm has many advantages over existing single key image algorithms such as bit plane crypt and edge map crypt algorithms. The security concern has been improved effectively. It is very easy to implement in hardware because they operate at the binary levels. They are also suitable for multimedia protection in real-time applications such as wireless networks and mobile phone services.

References

[1] Pommer, A. Uhl, "Image and video encryption: from digital rights management to secured personal communication", Advances in Information Security, Vol. 15, 161p., 2005

[2] B. Schneier.: Cryptography: Theory and Practice, CRC Press, Boca Raton, 1995.

[3] Yong Feng, Xinghuo Yu, “A Novel symmetric image encryption approach based on an invertible two dimensional map”. 35th Annual Conference on Industrial Electronics, pp.1973-1978, 2009.

[4] Kuang Tsan Lin, "Hybrid encoding method by assembling the magicmatrix scrambling method and the binary encoding method in image hiding", Optics Communications, Vol. 284, pp. 1778-1784, 2011.

[5] Anil Kumar and M. K. Ghose, "Extended substitution-diffusion based image cipher using chaotic standard map", Communication in Nonlinear Science and Numerical Simulation, Vol.16, Issue 1, pp. 372-382, 2011.

[6] Zhi-liang Zhu, Wei Zhang, Kwok-wo Wong and Hai Yu, "A chaosbased symmetric image encryption scheme using a bit-level permutation", Information Sciences, Vol. 181, pp. 1171-1186, 2011.

[7] Kamlesh Gupta and Sanjay Silakari, "Novel Approach for fast Compressed Hybrid color image

Cryptosystem", Advances in Engineering Software, Vol.49, pp. 29-42, 2012.

[8] Qiudong Sun, Wenying Yan, Jiangwei Huang and Wenxin Ma, "Image encryption based on bit-plane decomposition and random scrambling". 2nd International Conference on Consumer Electronics, Communications and Network, pp. 2630-2633, 2012.

[9] Y. Zhou, K. Panetta, S. Agaian and C. L. Philip Chen, "Image encryption using P-Fibonacci transform and decomposition", Optics Communications, Vol. 285, pp. 594-608, 2012.

[10] A Linfei Chen, Daomu Zhao and Fan Ge, "Image encryption based on singular value decomposition and Arnold transform in fractional domain", Optics Communications, Vol.291, pp. 98-103, 2013.

[11] V S Giridhar Akula, “A Novel Approach to Encrypt and Decrypt Color images”, Asian Journal of Computer Science and Technology, The Research Publication, Vol.4, No.2, 2015, pp. 13-17.