IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. V (Mar – Apr. 2015), PP 07-15
www.iosrjournals.org

DIP Using Image Encryption and XOR Operation Affine Transform

Anurag Singh[1], Dr. Namrata Dhanda[2]
[1](Research Scholar/ Department of Computer Science / GITM, Lucknow)
[2](Associate Professor/ Department of Computer Science / GITM, Lucknow)

Abstract: *Digital image processing is the use of computer algorithms to perform image processing on digital images. It is a subfield of digital signal processing. Digital image processing has many advantages over analog image processing; it allows a much wider range of algorithms to be applied to the input data, and can avoid problems such as the build-up of noise and signal distortion during processing. Since images are defined over two dimensions digital image processing can be modeled in the form of Multidimensional Systems.*
Images are produced by a variety of physical devices, including still and video cameras, x-ray devices, electron microscopes, radar, and ultrasound, and used for a variety of purposes, including entertainment, medical, business (e.g. documents), industrial, military, civil (e.g. traffic), security, and scientific. The goal in each case is for an observer, human or machine, to extract useful information about the scene being imaged.
An image is defined as a two-dimensional function, f(x, y), where x and y are spatial coordinates, and the amplitude of f at any pair of coordinates (x, y) is known as the intensity or gray level of the image at that particular point. The image is known as digital image when x, y, and the amplitude values of f are finite and discrete values. Processing of digital images by means of a digital computer is done in the field of Digital Image Processing. A digital image constitutes a finite number of elements, each of which has a particular location and a particular value. These elements are called picture elements or image elements or pels or pixels. Pixel is the term most widely used to denote the elements of a digital image
Keyword: *Arnold Transform, Affine Transform, Block Level XOR Operation, Exclusive-OR (XOR)*

I. Introduction

Digital image processing is the use of computer algorithms to perform image processing on digital images. It is a subfield of digital signal processing. Digital image processing has many advantages over analog image processing; it allows a much wider range of algorithms to be applied to the input data, and can avoid problems such as the build-up of noise and signal distortion during processing. The main idea in the image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. The image information has special properties such as bulk capability, high redundancy and high correlation among the pixels that imposes special requirements on any encryption technique.

II. Overview Of Image Encryption

Image encryption is necessary for future multimedia Internet applications. Password codes to Identify individual users will likely be replaced are biometric images of fingerprints and retinal scans in the future. However, such information will likely be sent over a network. When such images are sent over a network, an eavesdropper might duplicate or reroute the information. By encrypting these images, a degree of security can be achieved. Furthermore, by encrypting noncritical images as well, an eavesdropper is less likely to be able to distinguish between important and non-important information. Encryption is also used to protect data in transit, as an Example data being transferred via networks (e.g. the web, e-commerce), mobile telephones, wireless microphones, wireless communication systems, Bluetooth devices and bank automatic teller machines.

The main idea in the image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. The image information has special properties such as bulk capability, high redundancy and high correlation among the pixels that imposes special requirements on any encryption technique.

Image encryption can also be used to protect privacy. As an example for image encryption to protect privacy is in medical imaging applications. Recently, in order to reduce the price and to improve service, electronic forms of medical records have been sent over networks from laboratories to medical centers. According to the law, medical records, which include many images, should not be disclosed to any unauthorized persons. Medical images, therefore, should be encrypted before they are sent over networks.

Unlike the conventional cryptographic algorithms, which are mainly based on discrete mathematics, chaos-based cryptography is relied on the complex dynamics of nonlinear systems or maps, which are deterministic but simple. Chaotic maps present many desired cryptographic qualities such as simplicity of

implementation that leads to high encryption rates, and excellent security. Therefore, it can provide a fast and secure means for data protection, which is crucial for image data transmission over fast communication channels, like the broadband Internet communication.

Unlike text messages, image data have their special features such as high redundancy, and high correlation among pixels. Also, they are usually huge in size, which together makes traditional encryption methods difficult to apply and slow to process. Sometimes, image applications have their own requirements like real-time processing, fidelity reservation, image format consistence, and data compression for transmission, etc. Simultaneous fulfillment of these requirements along with high security and high quality demands has presented great challenges to real-time imaging practice. For studying image encryption, we must first analyze the differences between implementations for image data and text data. Basically, there are some differences between image and text as follows.

When the cipher text is produced, it must be decrypted to the original plaintext in a full lossless manner. However, the cipher image can be decrypted to the original plain image in some lossy manner. Text data are sequences of words. It can be encrypted directly by using block or stream ciphers. However, digital images are usually represented as 2D arrays. For protecting the stored 2D data, they must be converted to 1D array before using various traditional encryption techniques.

Since the storage space of a picture is very large, it's inefficient to encrypt or decrypt images, directly. One of the best methods is to only encrypt/decrypt information that is used by image compression for reducing both its storage space and transmission time.

III. Image Processing Operations

The processing of an image by means of a computer is generally termed as digital image processing. Image processing tasks can include any combination of the following:

3.1. Modifying the Image View

Transformation is an operation in image processing in which we study about the image from one space into other space, translating is the operation in which we move image up to some short of extent, while in rotation of a image involve rotate it to certain degree and resizing images in which we change image size, these are common tasks used to focus the viewer's attention on a specific area of the image.

3.2. Image Dimensionality

Some images provide more information when they are placed on a polygon, surface, or geometric shape such as a sphere.

3.3. Masks and Statistics

Image processing uses some fundamental mathematical methods to alter image arrays. These include masking, clipping, locating, and statistics.

3.4. Warping Images

Some data acquisition methods can introduce an unwanted curvature into an image. Image warping using control points can realign an image along a regular grid or align two images captured from different perspectives.

3.5. Specifying Regions of Interest (ROIs)

When processing an image, you may want to concentrate on a specific region of interest (ROI).

3.6. Manipulating Images in Various Domains

One of the most useful tools in image processing is the ability to transform an image from one domain to another. Additional information can be derived from images displayed in frequency, time frequency, Hough, and Radon domains. Moreover, some complex processing tasks are simpler within these domains.

3.7. Enhancing Contrast and Filtering

Contrasting and filtering provide the ability to smooth, sharpen, enhance edges and reduce noise within images.

3.8. Extracting and Analyzing Shapes

Morphological operations provide a means of determining underlying image structures. Used in combination, these routines provide the ability to highlight, extract, and analyze features within an image.

IV. Purpose Of Image Processing

The purpose of image processing is divided into several groups. Some of them are.

4.1. Visualization

Visualization's purpose is the communication of data. Which means that the information must come from something that is abstract or at least not immediately visible (like the inside of the human body).These rules out photography and image processing. Visualization transforms from the invisible to the. Visible Observe the objects that are not visible.

4.2. Image Sharpening and Restoration

Image restoration is the operation of taking a corrupted and noisy image and estimating the clean original image. Image restoration is different from image enhancement in that the latter is designed to emphasize features of the image that make the image more pleasing to the observer, but not necessarily to provide realistic data from a scientific point of view and to create a better image.

4.3. Image Retrieval

An image retrieval system is a computer system for browsing, searching and retrieving images from a large database of digital images. Seek for the image of interest. Searching and retrieving pictures from a large database of digital images.

4.4 Image Recognition

Image Recognition means the processing of the data of an image for comparing two images or components of images, stored in computer memory. It may be used, as an example, to identify fingerprints, or to interpret bar codes. Additionally referred to as pattern recognition, the identification of objects in an image. This method would in all probably start with image processing techniques such as noise removal, followed by (low-level) feature extraction to locate lines, regions and possibly areas with certain textures. One or Several pre-specified or learned objects or object classes can be recognized, typically together with their 2D positions in the image or 3D poses in the scene. Distinguish the objects in an image.

4.5 Image Authentication

The image information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

4.6. Image Encryption

Image encryption is an effective approach to protect images by transforming them into completely different formats. Which are used to protect the confidential image data from any unauthorized access .Several data encryption algorithms like Data Encryption Standard [8] and Advanced Encryption standard AES [9] are being employed for protecting digital information?

V. Various Image Encryption Methods

There are various types of image encryption methods. The image encryption algorithms can be categories into three major groups.

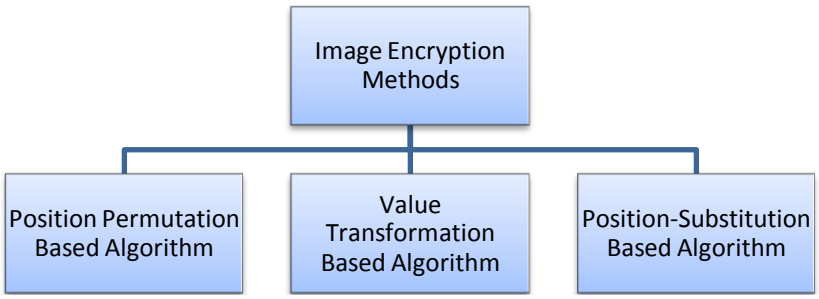


Figure 1 Various Image Encryption Methods.

- Position Permutation (Transposition) Based Algorithm.
- Value Transformation (Substitution) Based Algorithm.
- Position- Substitution Based Algorithm

5.1 Position Permutation (Transposition) Based Algorithm

Transposition means rearranging elements in the plain image. The rearrangement of element can be done by bit, pixel, and block wise. The permutation of bits decreases the perceptual information, whereas the permutation of pixels and blocks produce high level security. In the bit permutation technique, the bits in each pixel are permuted using the permutation keys with the key length equal to 8 (as the number of bits in each pixel). The number of permutations is = 8! = 40320 and the number of keys are 121. In the pixel permutation, 8 pixels are taken as a group and permuted with the same size key. The block size is (8 × 8) then it is difficult to decrypt. To extract the image, a combinational sequence of permutations and the permutation keys using pseudo random index generators should be known. In this investigation the combination of block, bit, and pixel permutation are used respectively. The Position Permutation Based Algorithm is use for the various techniques.

5.1.1 Mirror-like image encryption

The mirror-like image encryption algorithm based on a binary sequence generated from a chaotic system, an image is scrambled consistent with the algorithm. This algorithm consists of seven steps. Step- 1 determines a 1-D chaotic system and its initial point x (0) and sets k = 0. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates binary sequence from chaotic system. Steps-4, 5, 6, and 7 rearrange image pixels using swap function according to the binary Sequence. However this algorithm does not have any compression scheme and authenticity verification.

5.1.2 Chaotic image encryption

Chaotic image encryption proposed a new image encryption scheme based on a chaotic system. In their method, an unpredictable chaotic sequence is generated. It is used to create a binary sequence again. According to the binary sequence, an image's pixels are rearranged. This algorithm has four steps. Step-1 determines a chaotic system and its initial point x(0), row size M and column size N of the image f, iteration number no, and constants a , b, and c used to determine the rotation number. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates the binary sequence. Step-4 includes special functions to rearrange image pixels.

5.1.3 Arnold Transform

Arnold transform has periodicity and the transform is simple, but the periodicity depends on image size. The time of image recovery will be much long according to the periodicity.
Arnold transform is used widely in information hiding technology, but because of its long transform periodicity, it costs large time and computation memory. Arnold transform, also called cat map transform, is only suitable for encrypting N×N images. It is defined as-

$$\begin{matrix} x \\ y \end{matrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } M) \quad \ldots\ldots (3.1)$$

Where (x, y) and (x', y') are the pixel coordinates of the original image and the encrypted image, respectively. Let A denote the left matrix in the right part of equation (1), I(x, y) and I(x', y') (n) represent pixels in the original image and the encrypted image obtained by performing Arnold transform n times, respectively. Thus, image encryption using n times Arnold transforms can be written as.

$$I(x\ ,\ y)(k) = AI\ (x\ ,y)(k-1)(modN) \quad \ldots\ldots (3.2)$$

Where k = 1, 2, … , n, and I(x', y') (0) = I(x, y). Obviously, one can multiply the inverse matrix of A at each side of equation (2) to obtain I(x, y) (k −1). In other words, the encrypted image can be decrypted by iteratively calculating the following formula n times.

$$J(x\ ,y\ )(k) = A - IJ\ (x\ ,y)(k-1)(modN) \quad \ldots\ldots (3.3)$$

Where J(x', y') (0) is a pixel of the encrypted image, and J(x, y) (k) is a decrypted pixel by performing k iterations.

5.2. Value Transformation Based Algorithm

Values Transformation Based algorithm is based on the technique in which the value of each pixel is change to some other value. The new value of pixel is evaluated by applying some algorithm on pixel .Basically algorithm is mathematical computation where we take input as a pixel value compute it, with some formulas and produce a new value for that pixel . Value Transformation Based Algorithm are Digital Signatures and Lossless Image Compression and Encryption Using SCAN, Image Cryptosystems, Color Image Encryption Using Double Random Phase Encoding, Image Encryption Using Block-Based Transformation Algorithm and affine Transform etc.

5.2.1 Image Encryption using Digital Signatures

Image Encryption using Digital Signatures algorithm encrypts the image and embeds the digital signature into the image prior to transmission. This encryption technique provides three layers of security. In the first step, an error control code is used which is determined in real-time, based on the size of the input image. Without the knowledge of the specific error control code, it is very difficult to obtain the original image. The dimension of the image also changes due to the added redundancy. This poses an additional difficulty to decrypt the image. Also, the digital signature is added to the encoded image in a specific manner. At the receiver end, the digital signature can be used to verify the authenticity of the transmitted image. The advantage of the scheme is the authenticity verification. Increment in the size of the image due to added redundancy is the disadvantage of the algorithm.

5.2.2 Lossless Image Compression and Encryption Using SCAN

The methodology which performs both lossless compression and encryption of binary and gray-scale image . The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is a formal language-based 2 dimensional spatial-accessing methodology which can efficiently specify and generate a wide range of scanning paths or space filling curves. The disadvantage of the methodology is that compression encryption takes longer time. The distinct advantage of simultaneous lossless compression and strong encryption makes the methodology very useful in applications such as medical imaging, multimedia system applications, and military applications. The drawback of the methodology is that compression-encryption takes longer time.

5.2.3 Affine Transform

1. It is any transformation that can be expressed in the form of a matrix multiplication (linear transformation) followed by a vector addition (translation).
2. An Affine Transformation represents a relation between two images. We can use an Affine Transformation to express:

- Rotations (linear transformation) .
- Translations (vector addition) .
- Scale operations (linear transformation) .
- The usual way to represent an Affine Transform is by using a 2X3 matrix.

3. The usual way to represent an Affine Transform is by using a 2X3 matrix.

$$A = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix}_{2\times 2} \begin{bmatrix} b_{00} \\ b10 \end{bmatrix}_{2\times 1} \quad \text{.....(3.4)}$$

$$M = [A \quad B] = \begin{bmatrix} a_{00} & a_{01} & b_{00} \\ a_{10} & a_{11} & b_{10} \end{bmatrix}_{2\times 3}$$

4. The affine transform fractures the correlation between adjacent pixels of an image .Affine chipper is one-to-one mapping that is a symbol in the plaintext can be transformed to a unique symbol in the cipher text. In affine cipher, the relationship between the plain text C and the cipher text C is given in equations 1 and 2.

$$C = (K_0 - K_1 \times P) \bmod N \text{.....(3.5)}$$

$$\mathrm{P} = \left(\left(C + (-K_0) \right) \times K_1^{-1} \right) \bmod N \text{.....(3.6)}$$

5.2.4 Color Image Encryption Using Double Random Phase Encoding

A new method to encrypt color images using existing optical encryption systems for gray-scale images. The color images are converted to their indexed image formats before they are encoded. In the encoding subsystem, image is encoded to stationary white noise with two random phase masks, one in the input plane and the other in the Fourier plane. At the decryption end, the color images are recovered by converting the decrypted indexed images back to their RGB (Red-Green- Blue) formats. Since only one channel is needed to encrypt color images, it reduces the complexity and increases the reliability of the corresponding optical color image encryption systems.

5.2.5 Image Encryption Using Block-Based Transformation Algorithm

Block Based transformation technique works as follows: the original image is divided into a random number of blocks. Then these blocks get shuffled within the image. The generated (or transformed) image is then fed to the Blowfish encryption algorithm. The intelligible information present in an image is due to the correlation among the image elements in a given arrangement. So this technique reduced the correlation among the image elements using certain transformation techniques. The secret key of this approach is used to determine the seed. The seed plays a main role in building the transformation table, which is then used to generate the transformed image with different random number of block sizes. The transformation process refers to the operation of dividing and replacing an arrangement of the original image.

5.2.6 A chaos-based image encryption scheme

A chaos-based image encryption scheme was recently proposed and is widely referenced afterwards, but its security has not been analyzed efficiently. The encryption scheme is composed of two steps: chaotic confusion and pixel diffusion, where the former process permutes a plain-image with a 2D chaotic map, and the latter process changes the value of each pixel one by one. In the confusion process, the parameters of the chaotic map serve as the confusion key; in the diffusion process, such parameters as the initial value or control parameter of the diffusion function serve as the diffusion key. As shown in Fig. 2, the confusion and diffusion processes are both repeated for several times to enhance the security of this cryptosystem.

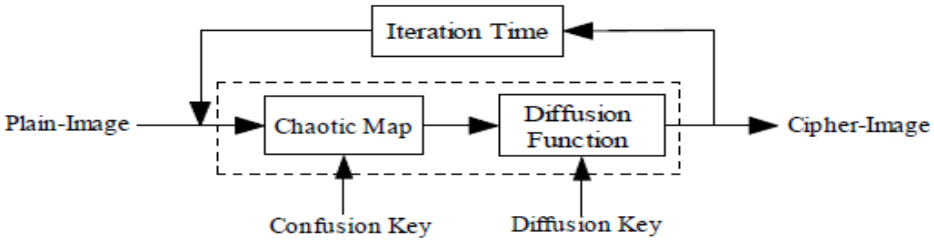


Figure 2. The chaos-based image encryption scheme. Here, the plain-image is encrypted into cipher-image through chaotic confusion, diffusion, and repeated iteration.

In the confusion process, many different 2D chaotic maps can be used, such as the Baker map, the Cat map and the Standard, which must be discretized over the image lattice to realize the confusion of all pixels.

5.3 Position- Substitution Based Algorithm

This technique is combination of both position permutation and value transformation. Position permutation and value transformation can be combined. In this technique first pixels are reordered and then a key generator is used to substitute the pixel values. The Position-Substitution Based Algorithm is use for the various techniques.

5.3.1 Image Encryption Based on Bit-plane Decomposition and Random Scrambling

The aim of this technique is to provides the positions interchange of pixels and their gray values change at the same time. In this technique a random scrambling algorithm based on bit-planes of image is used. At first, decomposed a gray image into several bit-plane images. Then shuffled them by a random scrambling algorithm separately. Lastly, merged the scrambled bit-plane images according to their original levels on bit-planes and gained an encrypted image.Experimental results show that the algorithm can not only scramble an image effectively, but also change its histogram apparently. This algorithm has better efficiency and properties than the general random scrambling method, and has more stable scrambling degree than the classical method like Arnold transform.

5.3.2 Image Encryption Using Affine Transform and XOR Operation

This technique uses two phase encryption symmetric key algorithm. It used a 64 bit symmetric key to encrypt a image. The 64 bits of key is divided into 8 sub-keys K0, K1, K2. K3, K4, K5, K6, and K7 of 8 bits each. The key is chosen is in such a way that the first sub-key is relatively prime to width of the image and the fourth sub-key is relatively prime to the height of the image .The reason for choosing this is because if the sub-keys are not prime to height and width of the image the transformation process may map more than one location to same destinations.

The first four sub-keys K0, K1, K2, K3 are used for location transformation of the pixel values of the image using affine cipher algorithm. Next four keys K4, K5, K6,K7 are used for second level of encryption using simple XOR operation. We use a location transformation of pixel values of the image because image data

has strong correlation among adjacent pixels. This strong correlation proves to be a weak point for any encryption algorithm. Anyone knowing a pixel value may predict the neighbor pixel values reasonably well using some prediction techniques. So, first of all, we break this correlation among image pixels by transforming them into new locations using affine transform.

5.3.3 Block Level XOR Operation

The exclusive or operation - a logical function applied to binary bits, like AND, OR, and NOT - is a fundamental encryption technique. It is often used in stream ciphers, which are widely used in web browsers when connecting to secure web servers.

When used properly, this technique provides strong protection. In fact, it is the basis for the one-time pad, the only provably uncrackable encryption. However, this protection is easily eroded if the cipher is not used correctly.

XOR is a trivial operation for computer logic to perform show the table 3.1. The operation often appears as a built-in machine instruction so that software can perform it in a single machine operation.

5.3.4 Exclusive-OR (XOR)

The following table shows how the XOR operation transforms individual bits. Let A be a bit from the plain text message, and B be a bit from the key. The ⊕ column shows the resulting bit.

Block Level XOR Operation, Exclusive-OR (XOR)

A	**B**	**⊕**
0	0	0
0	1	1
1	0	1
1	1	0

Table 1 Shows how the XOR operation transforms individual bits.

If A wants to send a secret message to B, it takes the sequence of bits in the message (the plain text) and a sequence of bits known only by it and B - the key. To encrypt, she combines the plain text and the key, bit by bit, using XOR. In a one-time pad, A and B must use a different set of secret, randomly generated bits for every message they exchange.

In a stream cipher, A and B share a much smaller number of secret bits and use them to generate a long, hard-to-guess sequence of bits. The stream cipher relies on a cryptographic algorithm to generate that long sequence from a small, shared secret. This generated sequence is then combined with the message using XOR.

For Example: Below we have the image message "Rose image" embedded in a 128 by128-bit image. For a key, we have collected a 128 by 128 matrix of random bits. We will combine the two matrices using XOR.

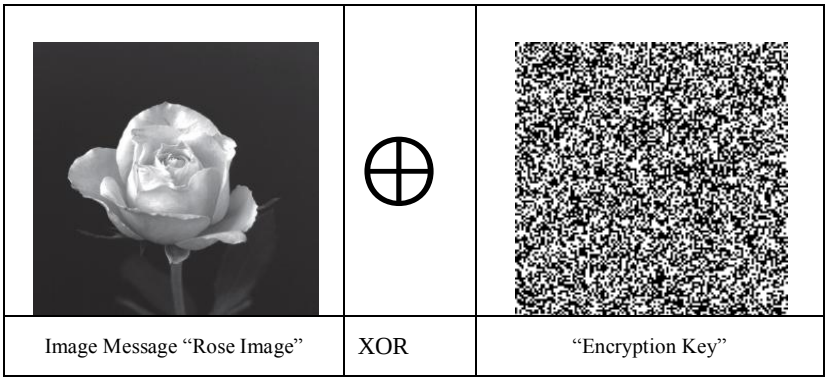
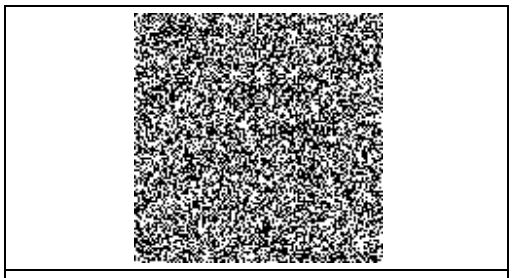


Figure 3 Send Rose Image Message Encrypted Key by using XOR Operation.

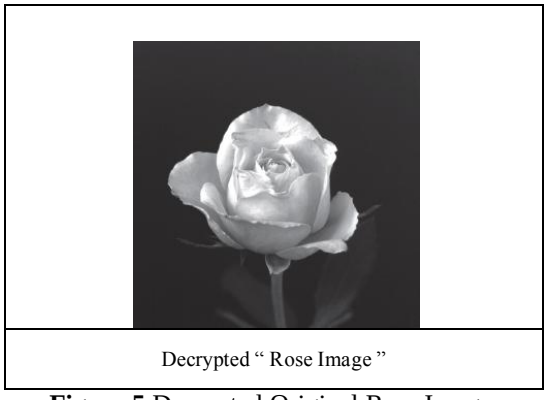
When we apply XOR bit-by-bit to the two matrices, we get the following 128 by 128 matrix of encrypted bits.



Encrypted " Rose Image "

Figure 4 Encrypted Rose Image.

To decrypt the message, we simply take the encrypted message and compute XOR with the encryption key, bit-by-bit. This yields the original image "Rose image" message.



Decrypted " Rose Image "

Figure 5 Decrypted Original Rose Image.

VI. Conclusion

In this work, the design and implementation of an encryption algorithm that provides both high **security** and **performance** were presented. Also, other features such as flexibility, simplicity and easiness of implementation are taken into account when designing the algorithm.

In this work, we proposed a symmetric key image encryption technique that first scramble the locations of the pixels using **4 8-bit sub keys** and then encrypt the pixel values by **XOR the selected 8-bit key**. The scrambling operation is done using Arnold transformation cipher techniques that breaks the correlations of the neighboring pixels and make the image unidentifiable. The XOR operation then change the pixel values making the image very meaningless. The encryption and decryption process are simple enough to be carried out on any large sized image or video files, but provides enough security. The proposed encryption method in this study has been tested on different gray images of 256*256 and showed good results. To accomplish this research work, We have designed our image Encryption and Decryption System using Matlab 7.8.0. We have evaluated our proposed image Encryption and Decryption System on gray Scale image.

Acknowledgement

I would like to thank my guide Dr. Namrata Dhanda, (Associate Professor, Department of Computer Science, GITM, Lucknow) who provided special assistance, support and encourage me by their thoughts, my special thanks to Goel Institute of Technology and Management, Lucknow.

References

[1]. D. L. B. Jupp, A. H. Strahler and C.E. Woodcock , "Autocorrelation and Regularization In Digital Images - Image Basic Theory", IEEE Transactions on Geosciences and Remote Sensing**, Vol.** 26, No. 4, pp. 463-473, 1988.
[2]. Amogh Mahapatra and Rajballav Dash, B.Tech Thesis On "Data Encryption And Decryption By using Hill Cipher Technique And Self repetitive Matrix", Department of Electronics & Instrumentation Engineering, National Institute of Technology ,Rourkela,2007.
[3]. B A Forouzan, Cryptography & Network Security , McGraw- Hill, India , 2007.
[4]. Castleman, K.R., Digital Image Processing. Second ed. 1996, Englewood Cliffs, New Jersey: Prentice-Hall.
[5]. Castleman, K.R., Digital Image Processing. Second ed. 1996, Englewood Cliffs, New Jersey: Prentice-Hall.
[6]. Dr. D. M. Shah, "Image Encryption & Decryption model".
[7]. F. Dachselt, K. Kelber and W. Schwarz, Chaotic Coding and Cryptoanalysis , Proceedings of IEEE International Symposium on Circuits and Systems, Hong Kong, pp. 1061-1064, 9-12 June, 1997.

[8]. Gonzalez, R.C. and R.E. Woods, Digital Image Processing. 1992, Reading, Massachusetts: Addison-Wesley. 716.
[9]. H Jin, Z. Liao, D. Zou, and C. Li, Asymmetrical Encryption Based Automated Trust Negotiation Model , The 2nd IEEE International Conference on Digital Ecosystems and Technologies (DEST 2008), pp. 363- 368, Feb. 2008.
[10]. H. Yu, Z. Zhu "An Efficient Encryption Algorithm Based on Image Reconstruction" 2009 International Workshop on Chaos-Fractals Theories and Applications.
[11]. Ian T. Young Jan J. Gerbrands Lucas J. van Vliet "Fundamentals of Image Processing", Delft University of Technology, version 2.3.
[12]. Image, Richard E. Woods, "Digital Image Processing", Prentice Hall Processing in IDL", IDL Publication Version 7.1 May 2009.
[13]. J. Wei, X. Liao, K. W. Wong and T. Zhou, Cryptanalysis of Cryptosystem Using Multiple One-Dimensional Chaotic Maps , Communications in Nonlinear Science and Numerical Simulation, In Press, pp. 814-822, 19 September 2005.
[14]. K.C. Ravishankar, M.G. Venkateshmurthy "Region Based Selective Image Encryption" 1-424-0220-4/06 ©2006 IEEE.
[15]. Michael Eziashi Osadebey , " Integrated Content-Based Image retrieval Using Texture, Shape And Spatial Information ", Master Thesis Report in Media Signal Processing, pp. 3-5 February 2006.
[16]. Mohammad Ali Bani Younes and Aman Jantan "Image Encryption Using Block-Based Transformation Algorithm" IAENG International Journal of Computer Science, 35,2008.
[17]. National Bureau of Standards, Data Encryption Standard Modes of Operation, Federal Information Processing Standards Publication 81, US Government Printing Office, Washington D. C, 1980.
[18]. National Institute of Standards and Technology, "Advanced Encryption Standards (AES)," http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
[19]. National Institute of Standards and Technology, "Data Encryption Standard (DES)," http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, 1999.
[20]. Payal Sharma, Manju Godara, Ramanpreet Singh ," Digital Image Encryption Techniques: A Review", International Journal of Computing & Business Research, 2012.

Author Profile:

Author (Anurag Singh[1]), is a research scholar in the field of Information Technology and Computer Science Engineering. He writes the 5 international research papers in his respected field in international reputed journals. He attend 5 national and 3 international seminars along with his studies.

Dr. Namrata Dhanda[2] is working as Associate Professor and Head of Department in the Department of Computer Science and Engineering/Information Technology at Goel Institute of Technology and Management, Lucknow. She has teaching experience of 14 years. Prior to her current assignment she has taught at Amity University, Lucknow and Babu Banarasi Das National Institute of Technology and Management, Lucknow at different positions. Her areas of interest include Automata theory, Database Management Systems and Algorithm design and Analysis.