A Survey on Image Encryption and Decryption using Blowfish & Watermarking

Preeti Gaur
Research Scholar,
Jagannath University,
Jaipur
gaurpreeti24@gmail.com

Neeraj Manglani
Asst. Professor,
Jagannath University,
Jaipur
neeraj.maglani@jagannathuniversity.or

Abstract- Internet means **Inter**national **Net**work. In the present era, to send and receive information, the internet is the main media. This information may be text, audio, graphics and video etc. There are many advantages of internet. Internet provides quickest data delivery services, security of data is major concern for all internet users. There is always a sense of insecurity amongst internet user after sending data or image until he gets an acknowledgment from the opposite side informing that they have received the data safely, that too without any manipulation in its content. The confidentiality, non-repudiation, validation, reliability, of the information (data or image) should be checked properly otherwise data manipulation can have big problem. We can get these objectives with cryptography which is simply the science of securing sensitive and confidential information as it is stored on media or transmitted through communication network paths. Here, images are considered with an aim to secure them during its storage and transmission. Blowfish Algorithm, a type of symmetric key cryptography is the best solution for this. The two processes, encryption and decryption together form the cryptographic process. For ensuring security, the images are encrypted by the sender before transmitting them and are decrypted by the receiver after receiving them so that only the sender and the intended person can see the content in the image. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular accessible algorithms. For double protection, after the blowfish process, the encrypted image tends to go through a water marking process which is used to hide a secret or personal message to protect a products copyright or to demonstrate data integrity Watermarking is the process of embedding new data into image, audio or video. We perform watermarking on different types of images say JPEG, BMP etc. The anticipated work is designed and implemented using MATLAB.

Keywords- Encryption, Decryption, Cryptography, Cryptology, Blowfish, Watermarking

*****

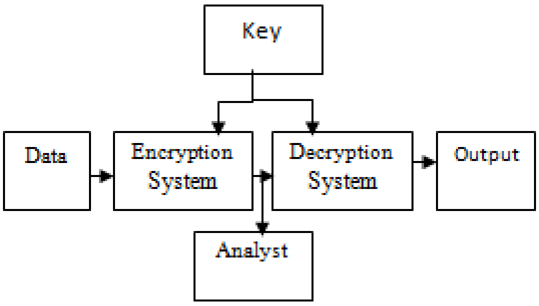
I. INTRODUCTION

To secure our data at the time of transmission cryptography gives an elucidation. Cryptography derived from a Greek word called “Kryptos” which means “Hidden Secrets”.

Cryptography can be defined as the art of safeguarding documents and it makes sure that only the intended people are able to perceive its data. It is essentially the facility of Science of converting a plain intelligible data and again retransforming that message into its original form.

The main five goals of Cryptography include privacy, Non -Repudiation, Service dependability and ease of use.

These objectives ensures that the private data remains private, the data is not altered illegally and assures against a party denying a data or a communication that was initiated by them.



Cryptosystem

Cryptosystem is the system that provides encryption and decryption. It uses algorithm for encryption and decryption. Data is provided to the encryption system with a key. In secure mode the same key is provided to the decryption system. Finally output is obtained after decryption.

BASIC TERMS USED IN CRYPTOGRAPHY

Plain Text: The original message which we wish to communicate with the others is defined as Plain Text. In cryptography the actual data which we send to the other is referred as Plain Text.

Cipher Text: The cipher text is the message which has been converted by the encryption algorithm. In cryptography the original message is transformed into non readable message.

Encryption: A process of converting plain text into cipher text is known as Encryption. Encryption algorithm and a key to send confidential data through an insecure channel is used in cryptography

Decryption: It is the reverse process of encryption. In this it convert the cipher into plain text. We require encryption algorithm and a key for decryption.

GOALS OF ENCRYPTION/DECRYPTION

Confidentiality: Information transmitted by the computer is accessed only by the authorized party.

Authentication: In this the identity of the sender is to be checked that whether the information is arriving from an authorized person or a false identity.

Integrity: To maintain the integrity of information only the authorized entity is allowed to modify the transmitted information.

Non Repudiation: Non Repudiation is the term in which deny the transmission is not allowed by the sender and the receiver of message.

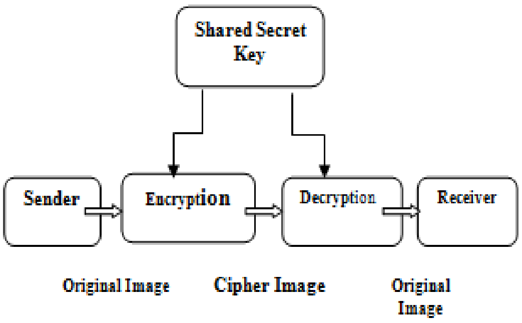
Access Control: Only the authorized parties can access the given information.

Cryptography is of two types:

1. Symmetric or Secret Key Cryptography
2. Asymmetric or Public Key Cryptography

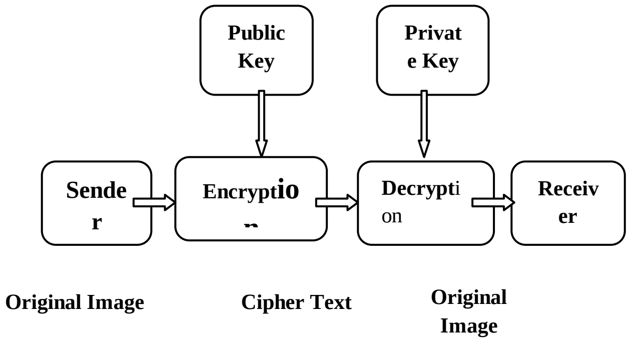
In Symmetric key cryptography, both the sender and receiver know the same secret code called key. In this cryptography the sender encrypted the message using the key and the receiver decrypts it using the same key.

E.g. : Triple DES, AES (Advanced Encryption Standard), (DES) Data encryption standard and Blowfish Encryption Algorithm.



Symmetric Key Cryptography

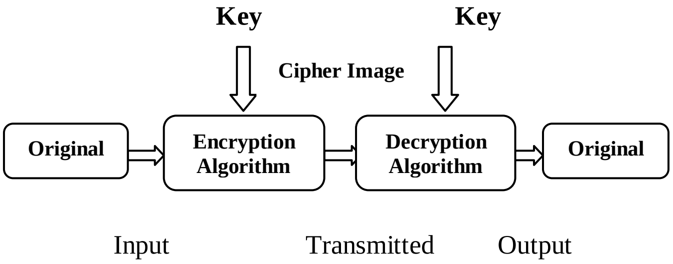
In Asymmetric key cryptography, different key is used by sender and receiver for encryption and decryption. The data is encrypted by sender using a public key and this key will be known by all the parties included in the communication. The data is decrypted by the receiver using a private key and it should be reserved as a secret. Example of asymmetric key cryptography is RSA.



Asymmetric Key Cryptography

Encryption is the process of transforming the information for its security. Image encryption techniques convert an image to another one that is not easy to understand. While, in image decryption the original image is retrieves from the encrypted one.

There are many image encryption algorithms which are available such as DES, RSA, AES, Blowfish, etc. but DES, RSA, AES have some disadvantages so Blowfish algorithm and watermarking process for image security is the best one. [1][3][4]



Encryption/ Decryption Algorithm

BLOWFISH ENCRYPTION

Blowfish has 16 rounds. The input is a 64-bit data element, x.
Divide x into two 32-bit halves: XL, XR.
Then, for i = 1 to 16:
XL = XL XOR Pi
XR = F (XL) XOR x R
Swap XL and XR
After the sixteenth round, swap XL and XR again to undo the last swap. Then, XR = XR XOR P17 and XL = XL XOR P18.
Finally, recombine XL & XR to get the cipher text. The figure shows the Process of encryption.

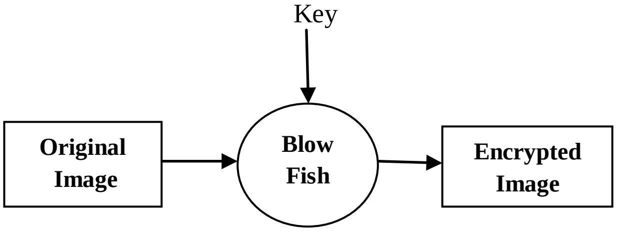


Image encryption using Blowfish Algorithm

BLOWFISH DECRYPTION

In this process, an already encrypted image is decrypted using the same key that was used at the time of encryption. This process is similar to encryption except that in decryption, P1, P2, … P18 are used in reverse order.

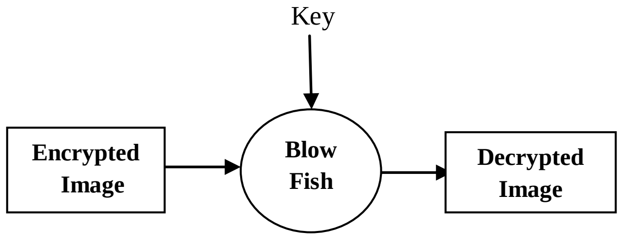


Image decryption using Blowfish Algorithm

WATERMARKING

Watermark

A watermark is a visible embedded overlay on a digital photo which consists of a logo, text or a copyright notice. The watermark is used to identify the work and discourage its unauthorized use.

Digital watermark

A digital watermark added to a photo, is more or less visible information in the form of a text or some other photo/image that has been added to the actual photo. The additional information can be less or more transparent to make it either easy or hard to notice the watermark.

Digital Watermarking

Digital Watermarking technique is used to hide a small amount of digital data in a digital signal in such a way that it can't be detected by viewer. A digital watermark is of two types-

I. Visible Digital Watermarking
II. Invisible Digital Watermarking

A **visible watermark** is a visible semi-transparent text or image overlaid on the actual image. In this the original image can be viewed, but by marking the image it still provides copyright protection as its owner's property. If we use a semi-transparent watermark placed over whole image then these watermarks are more vigorous against image transformation especially. So they are mostly used for strong copyright protection of intellectual property that's in digital format.

An **invisible watermark** is an embedded image which cannot be perceived by human's eyes. Hidden information to identify the copyright owner can be extracted only by electronic devices or specialized software. To mark a specialized digital content like text, images or even audio content to prove its authenticity, we use invisible watermark.

Typical applications of digital watermarking can include device control legacy enhancement, broadcast monitoring, proof of ownership, transaction tracking, content description, content authentication, and owner identification, copy control. [2]

II. LITERATURE SURVEY

Image encryption can be obtained by different methods. Some of important encryption methods are blowfish algorithm and digital watermarking. To know more about encryption following literature survey has done.

i) T. Sudha and B. Gopi proposed a image encryption technique in the paper **"Novel Spatial and Transform Domain Image Encryption Algorithms"**
In this paper three image encryption algorithms are proposed.

A) Spatial domain technique: - It performs spatial domain operations on image to hide the secret image in cover image.

B) Wavelet domain technique: - It hides the secret image in the decomposed data of cover image. The bits of decomposed data which can be retrieved by using other bits are used to hide the secret image.

C) Two stage encryption algorithm: - In the first stage the secret image should be decomposed into two share images. In the second stage the share images will be embedded in a cover image. The inverse operations will be performed to extract the secret image from the cover image. It is observed that the proposed techniques improve the security of secret image.

ii) Ashish Pant, Suneet Kumar Assistant Professor; Arjun Arora and Prof. R P Arora present a paper **"Sophisticated Image Encryption Using Open CV"**
In this paper, Image data structure of the Open CV has been analyzed in detail. In order to make various operations to the image data easily, we utilize the defined pointer to traverse all the image data. Combining with the existing Arnold transformation, the image has been encrypted. We use the inverse Arnold transformation for decryption .The library functions of Open CV make the encryption process simple and feasible, which lay a foundation for trying more updating operations. However, Arnold transformation is a complete and simple method of image encryption and the processing speed will become slow with increasing pixel data. In future, we can do better in improving the speed of encryption and decryption.

iii) **"A Generalized approach to Selective Image Encryption"** Anuradha Konidena, Neha Arora
In this paper we analyzed need of selective image encryption, which is followed by various mechanisms implemented by various research scholars for different kinds of data. The generalized approach is useful for real life applications which use multimedia data on devices which are low in resources. We would like to conclude that there is always tradeoff between level of security and cost of the algorithm.
Future Scope: This approach may further be extended to handle multiple images/pictures simultaneously

iv) **"Digital Watermarking Using MATLAB"** Pooya Monshizadeh Naini
In this chapter, implementation of basic digital watermarking methods in MATLAB is described.

Fundamental methods in spatial, spectral, and hybrid domains are described and
sample codes are given. Finally, some solutions for qualifying the watermarking method are described

v) "**Guarding Images using a Symmetric key Cryptographic Technique: Blowfish Algorithm"** Dr. J. Abdul Jaleel, Jisha Mary Thomas
The inputs selected with an aim to encrypt and decrypt include a gray scale image of Lena in PNG format and a color image of a cute baby in JPG format. The image processing part was done using MatLab and the encryption-decryption part was coded using VHDL. The results show that the encrypted image provides no information about the original image and the decrypted image is almost an exact replica of the input image. The Blowfish algorithm is strong and immune to hacking as it encrypts the data by a 16 round function iterating Feistel network

vi) "**Image Security using Encryption based Algorithm"** Ratinder Kaur, V. K. Banga
In this paper, a better method has been proposed for image security using a combination of block based image transformation and encryption techniques. The result showed the image security by using the block based transformation method before applying the encryption technique. Correlation was decreased when the proposed method was applied to them before the Blowfish algorithm. The proposed algorithm has the best performance; the lowest correlation and the highest entropy

vii) **"Image Encryption And Decryption Using Blowfish Algorithm In Matlab"** Pia Singh
Prof. Karamjeet Singh
Both color and black & white image of any size saved in tagged image file format (TIF), Bit map (bmp), Portable network graphics (PNG), Joint Photographic Experts group (jpg), etc. can be encrypted & decrypted using blowfish algorithm. Histogram of encrypted image is less dynamic and significantly different from the respective histograms of the original image. Blowfish cannot be broken until an attacker tries 28r+1 combinations where r is the number of rounds. Hence if the number of rounds are been increased then the blowfish algorithm becomes stronger. Since Blowfish has not any known security weak points so far it can be considered as an excellent standard encryption algorithm.

viii) **"Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm"** Jasdeep Singh Bhalla, Preeti Nagrath
In this paper, a new technique of digital watermarking is proposed in which a watermark is encrypted and embedded into another watermark and this combined watermark is embedded into the main image. This phenomenon of embedding one watermark into another is known as Nested watermarking. By doing so, the level of security of the watermark increases (due to use of encryption and decryption techniques) and the embedding capacity of the watermark is also enhanced (as concept of nested watermarks is used). The Blowfish encryption and decryption algorithm is used in this method as it is suitable and efficient for hardware implementation. Besides, it is unpatented and no license is required (Open source algorithm).

Advantages of this proposed method:

- ✓ Concept of Nesting increases embedding capacity of watermark into the main image.
- ✓ Encryption of watermarks before embedding them into main image helps to increase the security of the watermark.
- ✓ Use of Blowfish algorithm helps to make the method more robust.

III. CONCLUSION

From the survey it is concluded that the blowfish and watermarking techniques are the best techniques for image encryption. Both the techniques are having lots of features which give enhancement to the security methods.

REFERENCES

[1] International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 10, October 2014 "**Unique Key Using Encryption and Decryption of Image"** Kaladharan N Assistant Professor, Department of Electrical and Electronics Engineering, Annamalai University, India

[2] International Journal of Computer Science and Information Technologies, Vol. 3 (2), 2012, 3757-3760 "**Digital Image Watermarking for Copyright Protection"** Shankar Thawkar Department of Information Technology Hindustan College of Science and Technology, Mathura (UP), India

[3] Proceedings of National Conference on New Horizons in IT - NCNHIT 2013 "**Comparison Between DES, 3DES, RC2, RC6, BLOWFISH AND AES**" Milind Mathur, Ayush Kesarwani

[4] International Journal of Computer & Organization Trends – Volume 3 Issue 9 – Oct 20163 ISSN: 2249-2593 http://www.ijcotjournal.org Page 404 "**A New Approach For Image Cryptography Techniques"** Harpreet Singh, Dr.Naveen Dhillon, Sukhpreet Singh Bains M. Tech, Department of ECE, RIET, Phagwara, Punjab, India 2 HOD, Department of ECE, RIET, Phagwara, Punjab, India 3 AP, Department of ECE, RIET, Phagwara, Punjab,