STM JOURNALS

Journal of Artificial Intelligence Research & Advances
ISSN: 2395-6720 (Online)
Volume 4, Issue 3
www.stmjournals.com

Visual Cryptography Using Novel Algorithms

Diptanu Basak, Abhishek Das*
Department of Information Technology, Tripura University, Agartala, Tripura, India

Abstract

Encryption Schemes on images has tremendously increased to meet the demand of secure image transmission over various mediums such as Wired and Wireless Network. Various encryption standards show low efficiency over image encryption and have less impact on efficiency when the size of image is huge. Nowadays, secret communication plays a major role in many fields of mutual life, such as industry, banking and e-commerce etc. Due to the improvement in network expertise, information security becomes a current application of multimedia technology and swelling communication skill of network progressively leads us to obtain information directly and evidently through images. Hence, data security has become a serious issue. It is a crucial concern that proper encryption decryption should be applied to transmit the data from one place to another place across the internet in order to prevent unauthorized access. Image Cryptography is a special kind of encryption techniques to hide data in an image for encryption and decryption of original message based on some key value. Very few algorithms, provides computational hardness and it makes difficult to break a key to find the original message. In this paper, a variant of the RSA algorithm is used to encrypt the image files to enhance the security in the communication area for data transmission. An image file is selected to perform encryption and decryption using key generation technique.

Keywords: *Visual Cryptography, Encryption, RSA Algorithm*

****Author for Correspondence*** E-mail: adas@tripurauniv.in

INTRODUCTION

We have seen that from the last few years an increase in demand of data communication over the internet. For data communication over the internet it is very important that the data should be securely transmitted. Therefore, we use secure transmission by using cryptography. Security and authenticity are the two main issues with transferring data over internet. The security mainly protects data from attackers or hackers. There are many ways to transfer data over internet like email, facebook, twitter etc. Recently images are more using for transmitting over the internet. Image Encryption is the best way to secure the information. Image Encryption is the technique of converting the original image into another format using an encryption technique. Same way in the decryption, no one can retrieve the information without knowing the decryption key.

Image Encryption mechanism also allows only the authorize receiver to read the original message which the sender sends. This mechanism is commonly called as cryptography. There are many number of algorithms specially made for secure communication. It consists of two processes enciphering which will be done on sender side and deciphering which will occur on receiver side. It must have some methods for authentication of a valid user, validation of data.

RSA is an algorithm that provides us the encryption and authentication system. This is developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is one of the first public key cryptosystems and it is widely used for securing the data transmission. In this cryptosystem, the encryption key is a public one and the decryption key is a keep secret. RSA is an asymmetry cryptography, which is based on the product of two large prime numbers, the factoring problem. The RSA encrypt key is to encrypt the image, so that it converts into cipher text format and it will be stored as a text file. The opposite method of encryption is to execute by using one decryption key of RSA algorithm and it decrypts the image from

the cipher text. Finally, it will discover the resultant image by the decryption techniques. In this method height and width of both encrypted and decrypted image is same.

RELATED WORK

Creating a robust watermarking algorithm with high level of robustness to geometrical, noising, denoising and image processing attacks along with better PSNR (Peak Signal to Noise Ratio) [1]. Problem of copyright violation of digital media like images, audio clips, videos etc.; Internet has increased illegal transfer, copy, manipulation and redistribution of digital media [1].

In another paper, Mahesh et al. [2] proposed encryption scheme operates on both the image pixel values and the image frequencies in a loss less manner. The algorithm is a modification of an encryption scheme using Discrete Haar wavelet transform.

Security due to high level of confusion and diffusion makes the level of security in high range and also maintains the privacy of the data. To do these, make the keys and ciphers more complex for strong security [3]. Data of encrypted image are modified for data embedding, a direct decryption can still result in the original plaintext image and the error-correction mechanism used to ensure successful data extraction and perfect image recovery [4]. In another paper, Bhowmik and Acharyya [5] analyzed the application of Genetic Algorithm for image security using a combination of block-based image transformation and encryption techniques.

Chaotic DDE attractor image is generated in extremely small change in the initial conditions or in the time constant will result in largely chaotic behaviors [6]. Handling multimedia system information size is sometimes terribly massive [7] and requires to be processed within real time, only numerically calculated values might not be enough for similarity assessment and human observation might be required [8]. Compress the image to reduce the execution time of encryption-decryption using magic rectangle (MR) [9]. When there are possible losses during transmission, extracted bits in Share 1 and Share 2 may be affected, and the stacked result may fail to provide recognizable characters [10]. In another paper Maksuanpan and San-Um [11], proposed cryptography technique attempts to achieve simple-but-highly-secured image encryption and decryption algorithms in a category of chaos-based cryptosystems. In the paper Shun [12] proposed a method of modulation and demodulation in communication system; this paper presents a unique and useful way to protect the information of image in transmitting.

The secret image needs MxNxCxB BIT of memory is required to store in bitmap format with height (M), width (N), number of color components (C), and number of BITs (B) used to represent the pixel of each color component, respectively. The number of colors and the number of subpixels determine the resolution of the revealed secret image. If the number of colors is large, coloring the subpixels will become a very difficult task [13]. The part of key generation and key exchange, ones the secure key is lost or regenerated this cryptosystem fails, takes more time for encryption and decryption process and the inefficient use of memory [14,15]. In another paper El_Deen et al. [16], used RSA cryptosystem which is one of asymmetric cryptosystems and the two symmetric systems, DES and Blowfish. When the value of prime numbers becomes smaller, the result becomes poor (not similar) to the original image [17].

In the paper Bhanji et al. [18] proposed a new methodology to detect the phishing website. Their methodology is based on the Anti-Phishing using visual cryptography. It prevents password and other confidential information from the phishing websites. Applying lossless image compression methodology to reducing the pixel expansion problem and maintain image quality [19]. In another paper Mohamed and Kadhim [20] proposed efficient and highly securable with high level of security and less computation using asymmetric RSA algorithm. In this maintaining the key is very important, if the key is lost then data will be lost effectively.

VISUAL CRYPTOGRAPHY

Visual Cryptography is an encryption technique that hide the visual information like

image, text etc. by converting into another form. Using this technique, images or data are available for only to selected people. Visual cryptography; also known as novel security method which is used to protect the image from unauthorized access of data and secures dissemination of sensitive information.

TYPES OF CRYPTOGRAPHY

Cryptography technique secures the secret message when it is transferred from one place to another place over the networks. The cryptography contains the two main categories which are following as,

A) Symmetric key cryptography
B) Asymmetric key cryptography

Symmetric Key Cryptography

Secret key cryptography is also known as symmetric key cryptography. In this type both the sender and the receiver know the same secret key. The sender encrypts the data or the information using the secret key and the receiver decrypts the information using the same secret key. In the symmetric cryptography the key is playing a very important role which depends on the key.

Asymmetric Key Cryptography

Asymmetric cryptography is used for encryption and decryption algorithm pair. With public key cryptography, keys work in pairs of matched public and private keys. Public key cryptography also called asymmetric key cryptography which is using a pair of keys for encryption and decryption. The drawback of symmetric cryptography is; if any third party somehow gets the key then he can disclose the information at any time. It overcomes with this technique where a separate private key is used for decryption which is not used in encryption.

FUNCTIONALITY OF IMAGE CRYPTOGRAPHY

The image cryptography works as per the flow chart which is shown in Figure 1. Figure 1 describes the step by step manner of processing in the encryption and decryption.

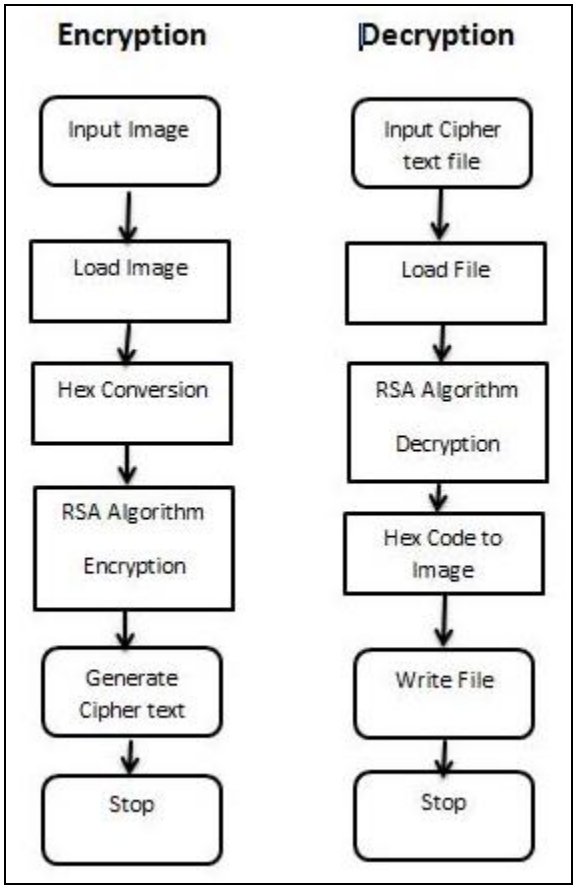

Fig. 1: *Encryption and Decryption Flow.*

IMAGE CRYPTOGRAPHY METHODOLOGY BY RSA

The RSA is a cryptographic algorithm which is used to encrypt and decrypt the data. This algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA cryptosystem is also known as the public-key cryptosystems. RSA is mainly used for secure data transmission over a network.

The encryption is starting on the RSA algorithm with the selection of two large prime numbers, along with an auxiliary value, as the public key. The prime numbers are keep in secret [18,20]. The public key is used to encrypt a message, and private key is used to decrypt a message or information. The RSA algorithm encrypts the original image and decrypts the image by the different keys. That is shown in Figure 2.

RSA ALGORITHM

RSA is an algorithm used in the modern computer environment to encrypt and decrypt the data in transform. The RSA algorithm is also called as an asymmetric cryptographic algorithm. Asymmetric cryptosystem means two different keys are used in the encryption and decryption.

In the two keys; one key is used for encryption and the second key is used for decryption. This RSA algorithm is also called as the public key cryptography because one of the secret keys can be given to everyone which means public. The other key must be kept private.

The RSA algorithm consists of three manor steps in encryption and decryption. The steps are following as,

A) Key Generation
B) Encryption
C) Decryption

Key Generation

The key generation is the first step of RSA algorithm. The RSA involves a public key and a private key. On those keys the public key can be known to everyone and it is used for encrypting messages. Messages encrypted with the public key can be decrypted using the private key. The keys for the RSA algorithm are generated by the following steps:

1) First choose the two distinct prime numbers p and q.
2) For security purposes, the integer p and q should be chosen, and it should be the similar bit-length. Prime integers can be efficiently found by a primality testing.
3) Then compute the n value, $n = pq$.
4) n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
5) Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where φ is Euler's totient function. This value is kept private.
6) Choose an integer e such that $1 < e < \varphi(n)$ and gcd $(e, \varphi(n)) = 1$; i.e., e and φ(n) are co-prime.
   e is released as the public key.
   e has a short bit-length and small hamming weight results in more efficient encryption.
   However, much smaller values of e have been shown to be less secure in some settings.
7) Determine d as $d \equiv e-1 \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo φ(n)). This is stated as, solve the d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$.

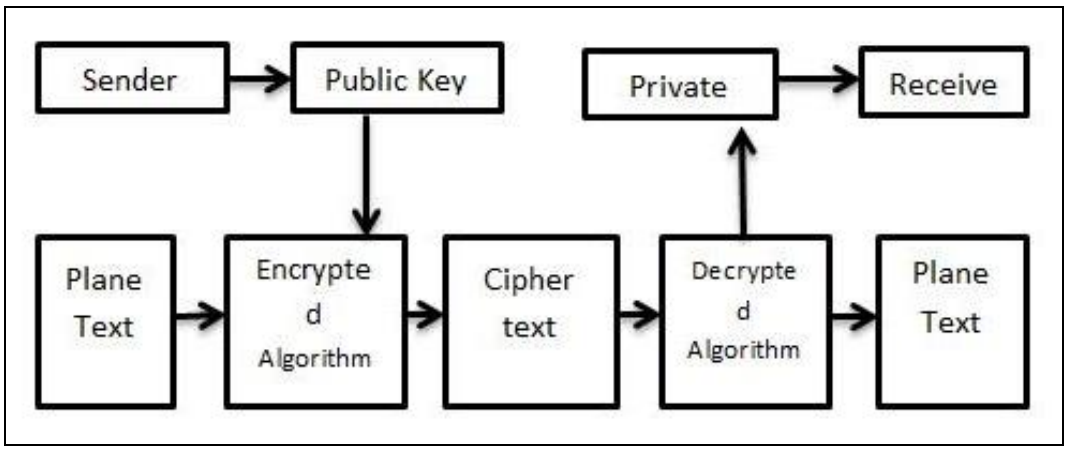

Fig. 2: *RSA Diagram.*

This is computed using extended Euclidean algorithm. It is using the pseudo code in the Modular integers section, inputs a and n correspond to e and φ(n), respectively.

8) d value is keep as the private key.

The public key consists of the modulus n and the public key e. The private key has the modulus n and the private key d, and it keep in secret. p, q, and φ(n) values are keep in secret, because they can be used to calculate d.

Encryption

'A' transmits his public key (n, e) to 'B' and keeps the private key d secret. 'B' then it is wish to send the message M to 'A'. So, first turns M into an integer m, such that $0 \leq m < n$ and gcd(m, n) = 1. Then it computes the cipher text c.

This can be done efficiently, even the numbers are 500-bit numbers and it is using the Modular exponentiation. 'B' then transmits c to Alice. At least nine values of m will yield a cipher text c equal to m.

Decryption

'A' can recover m from c by using private key exponent d via computing. Given m, she can recover the original message M by reversing the padding scheme.

APPLICATIONS OF IMAGE CRYPTOGRAPHY

Core banking is a set of services providing by the group of networked bank branches. Bank customers may access their funds and perform the simple transactions from the member branch offices. The major issue in core banking is the authenticity of the customer. An unavoidable hacking of the databases on the Internet, it is always quite difficult to trust the information in Internet. To solve this problem of authentication proposing an algorithm based on image processing and image cryptography.

The internet multimedia applications are becoming popular. The valuable multimedia content such as the image is vulnerable to unauthorized access while in storage and during transmission over a network. The image processing applications have been commonly found in the Military communication, Forensics, Robotics, Intelligent systems etc.

CHARACTERISTICS OF AN IMAGE CRYPTOSYSTEM

For studying characteristics of image encryption, the first step is to analyze the implementation differences between image and text data.

1) During the encryption process of text data, the decrypted text must be equal to the original text in a full lossless manner. However, this requirement is not necessary for image encryption; the cipher image can be decrypted to an original image in some lossy manner.
2) Text data are sequence of words which can be encrypted directly by using block or stream ciphers. However, digital image data are represented as 2D array.
3) Since the storage space of a picture is very large, the process of encryption/decryption of the picture is very difficult. One of the best methods is image compression which reduces both its storage space and transmission time.

In general, there are three basic characteristics in the information field: privacy, integrity and availability. For privacy, an unauthorized user cannot disclose a message. For integrity, an unauthorized user cannot modify or damage a message. As far as availability is concerned, message is made available only to the authorized users. An image cryptosystem cannot be called as a perfect cryptosystem even if it has a highly security mechanism, but it must also have elaborated overall performance.

The image security requires following characteristics:

1) The encryption system should be computationally secured. It requires an extremely long time to attack and any unauthorized user should not be able to read privileged image.
2) The security mechanism must be as widespread as
3) possible.
4) The security mechanism should be flexible.

5) There should not be a large expansion of encrypted image data.

EXPERIMENTS AND RESULTS

The experiment is made in Visual Studio 2010 C#.NET platform. In this paper, the cryptography mechanism is using the RSA algorithm with the public key encryption to increase the security levels of the encrypted. Here one key is needed to encrypt and another key is needed to decrypt the image. Finally, the image cryptography experiment is providing the feasibility of security to the image in network security. The data are not viewed by anyone without the knowledge of cryptography.

The image is consisting of secret and it is going to be encrypted, it is called as an original image may contain the data and it is shown in Figure 3.

The original image is encrypted by the key which is generated by the RSA algorithm. It is converting the image into the cipher text. It is shown in Figure 4.

Finally, the cipher text is decrypted by another decrypt key which is also generated by the RSA algorithm. And it converts the cipher text into the resultant image. It is shown in Figure 5.

Fig. 3: *Original Image.*

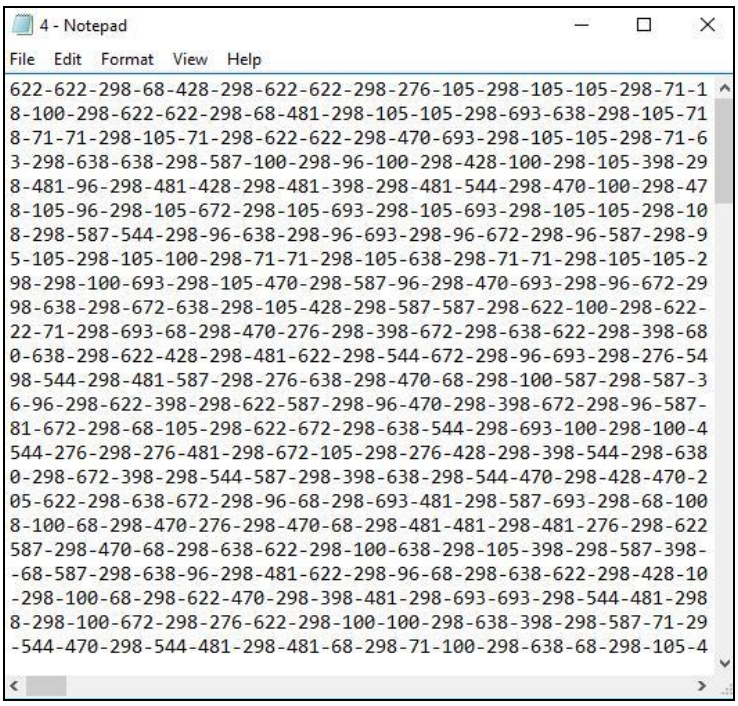

Fig. 4: *Encrypted Cipher Text.*

Fig. 5: *Decrypted Image.*

Now we will present the time of encryption and decryption of the algorithm for images with different sizes (Kb), the sizes of image which is used in simulation for images shown in Figure 6 present the time for both encryption and decryption algorithms for images and also size (Kb) of decrypted image.

The chart shown in Figure 7 presents the time for both encryption and decryption algorithms for images.

The chart below shown in Figure 8 shows difference between original image size and decrypted image size.

Image Name	Size of Orginal Image(KB)	Time required for Encryption	Time required for Decryption	Size of Decripted Image(KB)
Image1	27.7	3.58	1.51	15.9
image2	30.1	15.02	3.96	24.2
Image3	33.8	6.3	1.9	15.6
Image4	43.2	10.61	3.67	23.3
image5	46.3	58	15	48.1
Image6	62.3	13.17	3.84	23.3
Image7	80.6	75.6	19.11	53.4

Fig. 6: *Encryption and Decryption Time.*

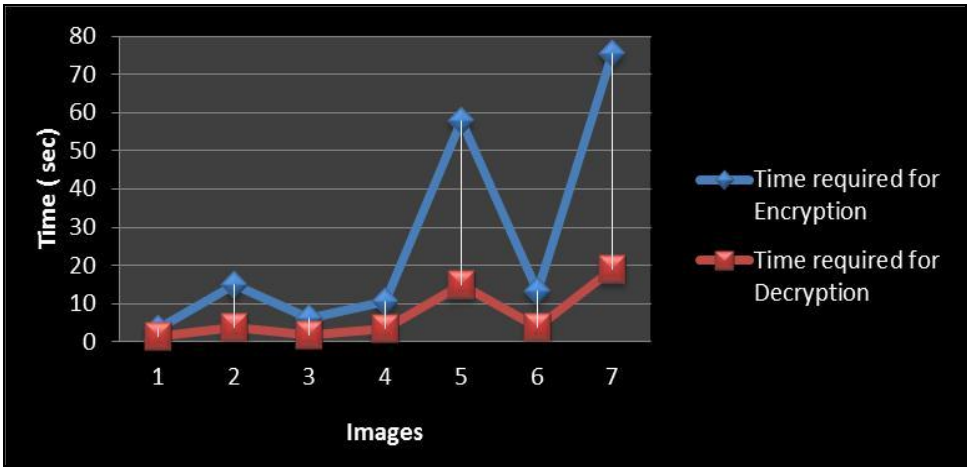

Fig. 7: *Chart of Time and Image in Encryption and Decryption Process.*

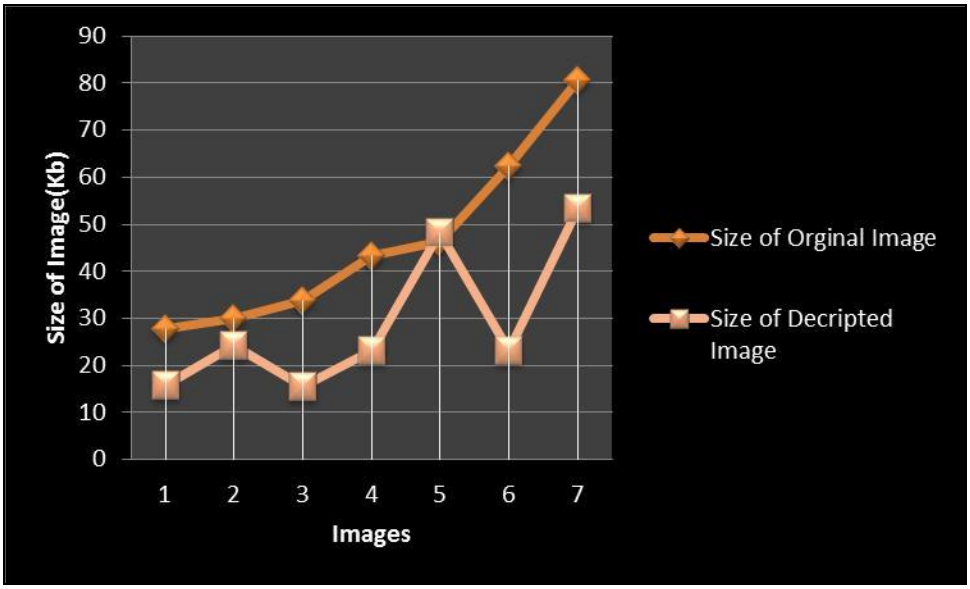

Fig. 8: *Chart of Original Image Size (Kb) and Decrypted Image Size (Kb).*

From these above charts and table, it is clearly seen that decryption time is always lesser than encryption time and the large image file is compressed into smaller with same resolution after decryption.

Output of the Image Encryption and Decryption Time before and after Compression using C#.net Platform

Before encryption:
File name: logo.jpg
Image resolution: 121 x121
Image size: 7,509 bytes
Encrypting Time: 1.012 sec
Encryption time: (As shown in Figure 9).
Decryption time: (As shown in Figure 10).

After decryption:
File name: logo2.jpg
Image resolution: 121 x121
Image size: 7,460 bytes
Decrypting Time: 0.785 sec

Following Functions are Part of the C# Program

Decode Hex: This function decodes the hex; means accepts hex string and converts it to byte array for image conversion.

IsPrime: This function checks parameter value, prime or not. This function is useful for validation purpose. Prime number accepts from user.

Convert Byte To Image: This function converts the byte array to image. Image is a bitmap image.

Convert Image To Byte: This function converts the image to byte array. Image is JPEG format image.

square: This function calculates the square value.

BigMod: This function is a recursive function. It calls itself. It works for encryption as well as decryption purpose.

n_value: This function calculates value of 'n'.

cal_phi: This function calculates phi, i.e., ϕ (n) value.

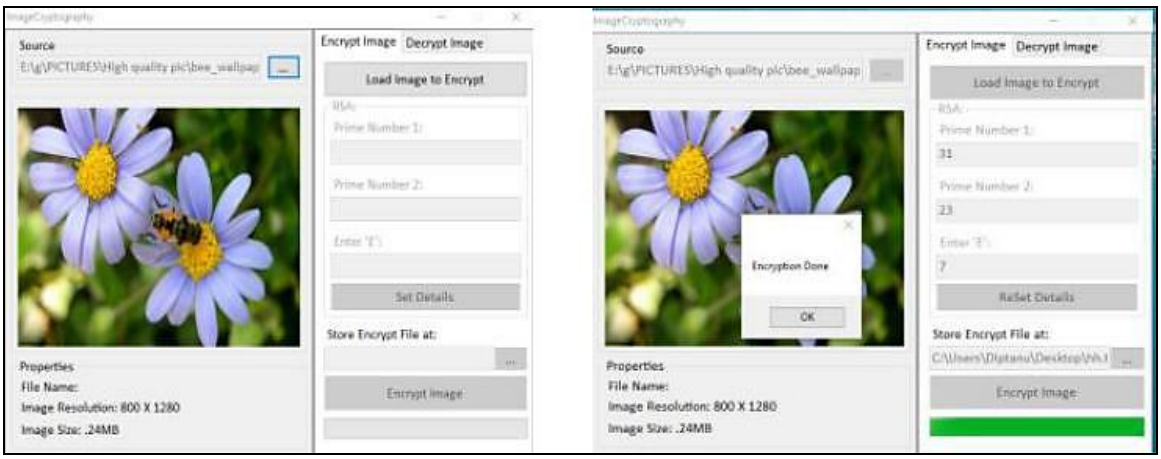

Fig. 9: *Output of Encryption Process.*

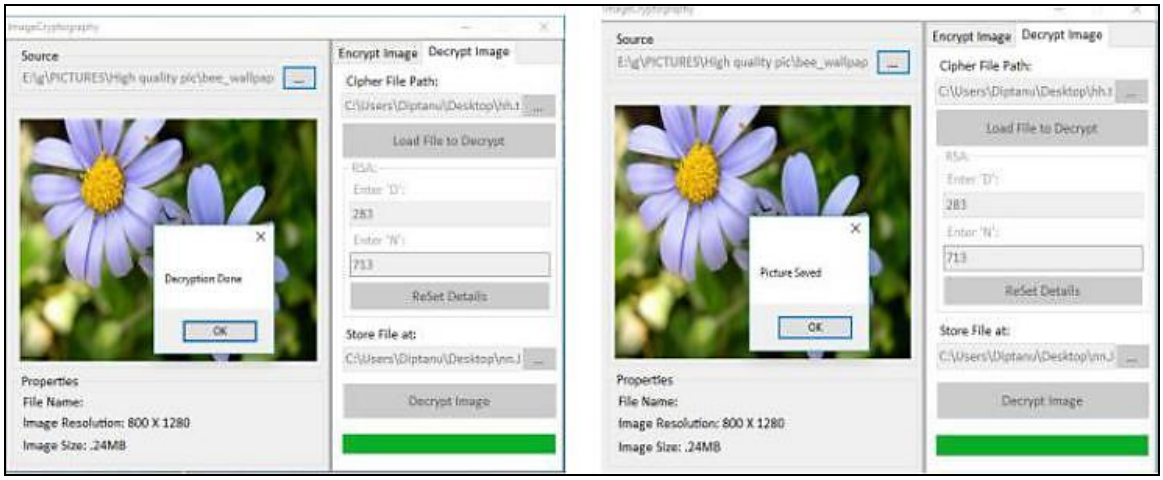

Fig. 10: *Output of Decryption Process.*

CONCLUSION

In the digital world, the security of images has become more important issue as the communication has increased rapidly. Here, the image encryption algorithm proposed efficient and highly securable with high level of security and less computation. The results of our experiments show that the algorithm has advantages based on the techniques which are applied on images. Hence it is concluded that the techniques are good for image encryption and give security in the open network. It has been observed that there are many possible enhancements and improved the visual quality and size of revealed image. The major areas of future scope are to improve the quality of decrypted images and reduce the time of computation.

REFERENCES

1. Sudip Ghosh, Sayandip De, Santi Prasad Maity, *et al.* A Novel Dual Purpose Spatial Domain Algorithm for Digital Image Watermarking and Cryptography Using Extended Hamming Code, *2nd International Conference on Electrical Information and Communication Technology (EICT), IEEE*, 2015, 169–172p.
2. Mahita Mahesh, Dhivya Srinivasan, Mila Kankanala, *et al.* Image Cryptography using Discrete Haar Wavelet transform and Arnold Cat Map, *IEEE ICCSP conference*, 2015, 1849–1855p.
3. Govinda K, Prasanna S. A Generic Image Cryptography Based on Rubik's Cube, *International Conference on Soft-Computing and Networks Security (ICSNS), IEEE*, Feb. 25–27, 2015.
4. Xinpeng Zhang, Jing Long, Zichi Wang, Hang Cheng, Lossless and Reversible Data Hiding in Encrypted Images with Public-Key Cryptography, *IEEE Transactions on Circuits and Systems for Video Technology*, 2016; 26(9): 1622–1631p.
5. Sandeep Bhowmik, Sriyankar Acharyya, Image Cryptography: The Genetic Algorithm Approach, *IEEE International Conference on Computer Science and Automation Engineering (CSAE)*, 2011, 223–227p.
6. Maksuanpan S, San-Um W. A New Simple Digital Image Cryptography Technique Based on Multi-Scroll Chaotic Delay Differential Equation, IEEE, *5th International Conference on Knowledge and Smart Technology (KST)*, 2013, 134–138p.
7. Niraj Kumar, Sanjay Agrawal, An Efficient and Effective Lossless symmetric Key cryptography algorithm for an Image, *IEEE, International Conference on Advances in Engineering and Technology Research (ICAETR)*, 2014.
8. Dipesh Shrestha, Sanjeeb Prasad Panday, Visual Cryptography using Image Pixel Transparency with Cover Image, *IEEE, 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*, 2015.
9. George DI Amalarethinam, Sai Geetha J. Image Encryption and Decryption in Public Key Cryptography based on MR, IEEE, *International Conference on Computing and Communications Technologies (ICCCT)*, 2015, 133–138p.
10. Hsiang-Cheh Huang, Feng-Cheng Chang, Visual Cryptography for Compressed Sensing of Images with Transmission over Multiple Channels, IEEE, *International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, 2015, 21–24p.
11. Maksuanpan S, San-Um W. A New Simple Digital Image Cryptography Technique Based on Multi-Scroll Chaotic Delay Differential Equation, IEEE, *5th International Conference on Knowledge and Smart Technology (KST)*, 2013, 134–138p.
12. Shun Da Lin, Image Transmission and Cryptography on the Basis of Mobius Transform, IEEE, *5th International Congress on Image and Signal Processing (CISP)*, 2012, 258–261p.
13. Gopi Krishnan S, Loganathan D. Color Image Cryptography Scheme Based on Visual Cryptography, IEEE, *International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN)*, 2011, 404–407p.

14. Jun He, Jun Zheng, Color Image Cryptography using Multiple One-dimensional Chaotic Maps and OCML, IEEE, *International Symposium on Information Engineering and Electronic Commerce*, 2009, 88–89p.
15. Kunal Jain, Jitender Singh, Rushikesh Kapadnis, *et al.* Effective Cryptposystem using MRGA with Steganography, *Int J Adv Res Comp Commun Eng.* March 2015; 4(3): 330–332p.
16. Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran, Digital Image Encryption Based on RSA Algorithm, *IOSR-JECE*. Jan. 2014; 9: 69–73p.
17. Asha Bhadran R, An Improved Visual Cryptography Scheme for Colour Images, *IRJET*. Aug-2015; 02(05): 1391–1395p.
18. Aboli Bhanji, Priyanka Jadhav, Sayali Bhujbal, *et al.* Secure Server Verification by Using RSA Algorithm and Visual Cryptography, *IJERT*. April – 2013; 2(4): 2340–2347p.
19. Ketan Raju Kundiya, Ram B. Joshi, Secure System Framework for Secure Visual Cryptography, *Int J Comp Appl.* January 2015; 109(14): 5–7p.
20. Rand Mahmoud Mohamed, Alaa Kadhim, Visual Cryptography for Image Depend on RSA & AlGamal Algorithms, IEEE, *Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, Iraq, May 2016.

AUTHOR'S BIOGRAPHY

Dr. Abhishek Das is currently working as an Asst. Professor in the Dept. of Information Technology, Tripura University (A Central University), India. His Research Area is in Medical Image Processing, Computer Vision and IoT. He has worked previously as a Reader in Computer Sc. & Engineering, Indian Institute of Space Science & Technology (IIST) and Lecturer in Information Technology, Bengal Engineering and Science University, Shibpur (now IIEST Shibpur) His Ph.D is from the Dept. of Computer Sc. & Engineering, Jadavpur University, India. His M.S. in Electrical & Computer Engineering from Kansas State University, USA and B.Tech in Computer Science & Engineering from Kalyani University, India. He has worked as a Business System Analyst in Blue Cross Blue Shield New York, USA & as a Quality Analyst in Vensoft Inc. Phoenix, USA and also as a Consultant Project Manager in the Software Industry. He is also a Visiting Scientist at Indian Statistical Institute, Kolkata. He has also worked in Technical Educational Administration as Regional Officer and Asst. Director (on deputation) at AICTE (under MHRD, Govt. of India). He is a NCERT National Scholar, New Delhi and a Tilford Dow Scholar, USA. His Biography has been published in the 28th edition of National Dean's List, USA. He is a Member of IEEE and a Honorary Senior Member of IACSIT Singapore. He has several publications in International and National Journals and peer-reviewed Conferences. He is also a TPC Committee Member of IEEE International Conferences in South-East Asia and Editor of the Journal on Image Processing and Computer Vision of IGI Global Publishers, USA (SCI and Scopus Indexed).

Cite this Article

Diptanu Basak, Abhishek Das. Visual Cryptography Using Novel Algorithms. *Journal of Artificial Intelligence Research & Advances*. 2017; 4(3): 1–10p.