Stream Encryption Standard for Digital Images

Akhil Kaushik, Satvika Khanna, Manoj Barnela and Anant Kumar

Abstract—**Present era is the information age where information is money and its security is the primary concern. If the organization has faster access to accurate and up-to-date information then correct business decisions can be taken in time to achieve business excellence and uphold an edge over competitors. Various kinds of security mechanisms like cryptography and steganography are extensively employed to keep the information secure and to send it over the network. However cryptography approach is more widely implied than steganography approach because of enhanced security and simplicity. Fundamental goal of any cryptographic algorithm is to provide defence against unauthorized attacks. In this paper, we have proposed a new image encryption algorithm named Stream Encryption Standard for Digital Images (SES) for meeting the requirements of secure image transfer. The results of several experimental and statistical analysis demonstrate that the proposed image encryption scheme provides a proficient and secure way for image encryption. This new algorithm is based on the symmetric key encryption approach.**

Index Terms—**Stream cipher, SES, Cryptography, Decryption, Encryption, Symmetric key algorithm.**

I. Introduction

The image is more lively, visual and expressive than standard text data and hence they are an important means of communication for the humans. With the incessant development of Internet and World Wide Web, sending and receiving images over the network have increased dramatically over the past decade. Security of these images becomes even more critical when they are confidential military data, new style weapon photograph, medical images/x-rays, or architectural charts of financial institutions. Plenty of safety approaches are available to transfer images within the organization's premises. But when images need to be transferred over the network outside company's premises, then there is a need of a protection technique which is not only secure but also efficient for transferring the images quickly. This technique can be broadly classified into two categories: Steganography and Cryptography. Steganography can be described as the technique for hiding a secret message within a larger one such that no one except the sender and receiver suspects the contents or even the existence of the hidden message[6]. This approach has been used since ancient times; for example Greek kings used to tattoo secret information on slave's head and then hide it by growth of his hair. Later information was retrieved by shaving his head at the receiving end. However, steganography is not vastly popular and rarely used these days.

Most famous and widely used approach for secure communication is "Cryptography" which is the practice and study of hiding information. Cryptography word is derived from the Greek word *kruptos*, meaning "hidden". It is normally also referred as "Encryption", which is used to disguise data, making it unintelligible to unauthorized observers[2][3]. Decryption is the reverse process i.e. moving from the unintelligible cipher text back to plaintext. The main advantage of cryptography is that communication between both sending and receiving ends remains inconceivable by anyone who might be listening. Cryptography helps us to achieve three main security goals i.e. availability, confidentiality and integrity of the information. One example of cryptographic application is Enigma machine used by Germans during World War II to communicate safely within their defense forces and avoid eavesdropping. One way to classify cryptography is the key mechanism. Key can be defined as the rules which are responsible for converting plain text into cipher text. Depending upon the Key, cryptography can be alienated into two chief categories: Secret Key Cryptography and Public Key Cryptography[12]. Secret Key Cryptography uses same key (single key) for encryption and decryption of data, while Public Key Cryptography uses two mathematically related keys; one for encoding data at sending end and another for decoding data at receiving end. The former approach is simpler but distribution of secret key is the chief concern. The later approach is a bit complex due to two keys: private key and public key. The sender can use public key (available to everyone) of any individual or organization to send data and that data can only be decoded using the private key which is kept confidential (with the receiving person or organization) and thus making it more secure and widely accepted across the world[10]. Another nomenclature of cryptography takes in account the number of characters read in a single pass. First category is known as Block Cipher, which inputs a block of digits/ characters in a single pass and encodes it simultaneously. However this technique is faster but it may produce identical cipher texts for the same plaintext every time it is encrypted[3]. Second type is known as Stream Cipher, which encrypt plain text digits/characters one at a time. This technique is a bit slower than Block Cipher but is more secure as it produces different cipher texts every time.

Most of the existing encryption algorithms are normally suitable for the textual data and prove incompetent for the image encryption because of the inherent qualities of the image like visibility, high redundancy, abundance in information expression and strong correlations between neighboring pixels[5][7]. Moreover images are usually two-

Manuscript received September 8, 2010

Akhil Kaushik Masters of Information Technology,Central Queensland University, Melbourne, Post-3000, Australia (Email: akhil.kaushik@yahoo.com).

Satvika Khanna Assistant Professor, Computers Department,T.I.T&S College Bhiwani,Haryana, India,(Email: satvika16oct@gmail.com).

Manoj Barnela ,Assistant Professor, Electronics Department,T.I.T&S College ,Bhiwani, Haryana, India(Email: m.barnela@gmail.com).

Anant Kumar, B.Tech Final Year, Computers Engineering,T.I.T&S College ,Bhiwani, Haryana, India (Email: anant.beriwal@gmail.com).

dimensional as comparative to one-dimensional textual data and dimensional transformation must be taken into account before encrypting them. Image encryption technology encrypts images by pixel location scrambling and gray value transform to conceal the important information in the image[6]. It is a technique providing the protection based on image contents and offers the important assurance for safe transmission for image data. In this paper we have proposed a new Stream Cipher for encoding images named: Stream Encryption Standard for Digital Images (SES).

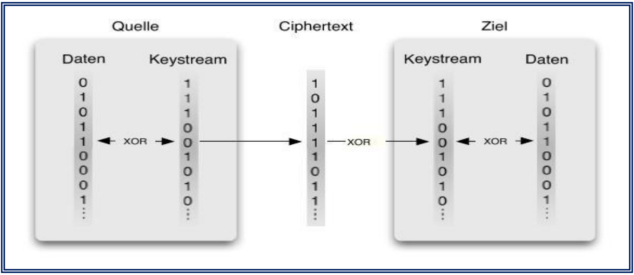

Figure 1: Block Diagram of a Stream Cipher

II. Proposed Symmetric Key Algorithm

This new proposed color image encryption algorithm is a stream cipher that encrypts each pixel using a special mathematical set of functions known as key. This algorithm uses same key at both sending and receiving ends i.e. it uses symmetric key methodology. Supplementary security measures are employed in algorithm to protect the secret key while sending it from one end to another. Thus, the key distribution predicament can be resolved with ease. SES algorithm also provides additional security against Brute-force attacks as the encryption key is altered many times during the encryption process and hence making it harder to get original image, even knowing or decrypting one key. SES algorithm will even protect against high redundancy of color images.

III. Encryption Procedure of SES

In this algorithm, a set of binary operations are performed like shift-left operation where we shift left to one place and MSB is shifted to LSB.

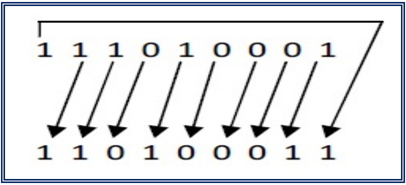

Figure 2. Shift Left Operation

These binary operations boost the security of the algorithm against eavesdroppers. Two predefined stacks have been used along with a logic based lookup concept. The first stack contains some specially chosen symbols, where other stack holds a random number from a given range by a predefined method to make the code sequence more secure[4].

The steps of encryption are given as follows:

A. The first pixel (starting from top left corner) of digital image is read from input file.

B. The RGB (red, green, blue) value of the pixel is read and changed into 24-bit binary number (8-bits each).

C. Then a special 8-bit number is appended to 24-bit number obtained in step ii.

D. Then shift-left operation is performed 10 times on this 32-bit number.

E. Now a secondary key of 32 bits is selected and XORed with output of step iv and stored as an intermediate cipher text. We make sure the output is of 32 bits only.

F. A random number is chosen from a given range and converted into 16-bit number.

G. A sequence symbol is selected from a predefined range.

H. The selected symbol is converted into ASCII code and then finally into binary number of 8 bits.

I. Result of step vii and viii are appended together to form a primary key.

J. Then with the help of preselected binary operations, primary key is applied to the intermediate cipher text to get the modified cipher text.

K. In next step, primary key is again applied to the output of previous step to generate new modified cipher text. This step is carried out 10 times to achieve the final cipher text of maximum 32 bits.

L. The first 8 bits of the final cipher text is discarded and remaining 24 bits are used to calculate RGB value of the resultant pixel.

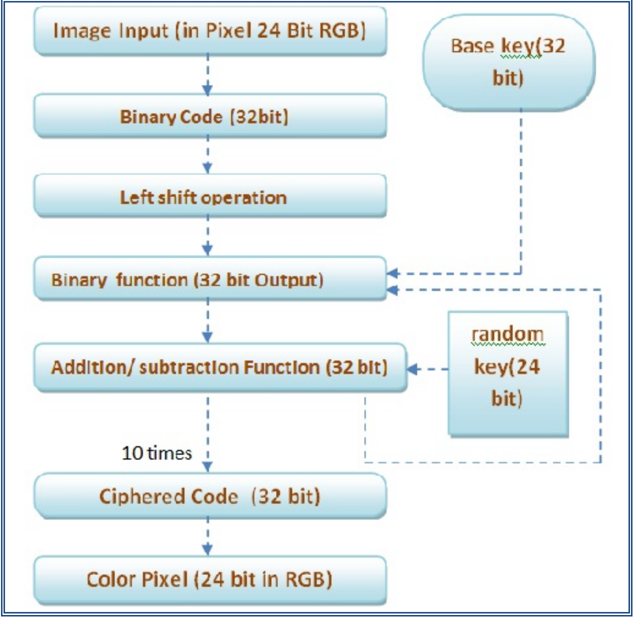
Image Input (in Pixel 24 Bit RGB)
Binary Code (32bit)
Left shift operation
Binary function (32 bit Output)
Addition/ subtraction Function (32 bit)
10 times
Ciphered Code (32 bit)
Color Pixel (24 bit in RGB)
Base key(32 bit)
random key(24 bit)

Figure 3. Block Diagram of SES Encryption Algorithm

IV. Decryption Procedure of SES

As SES algorithm uses symmetric cryptographic approach, so the decryption process in this algorithm is exactly the reverse of the encryption process.

A. The pixels of encrypted image are read from the received file and their corresponding RGB value is measured in binary form.

B. The respective key is read from the central database server.

C. Similar binary operations are performed on the cipher text with help of the key.

D. Steps ii to iii are performed 10 times to get the modified cipher text.

E. Reverse Binary operation is done on the modified cipher text with the help of secondary key.

F. Binary shift-right operation is performed ten times on the result of previous step.

G. Steps i to vi are repeated till the end of cipher text and output in binary form is stored.

H. The binary output is converted to the RGB value of the pixel to acquire the desired output.

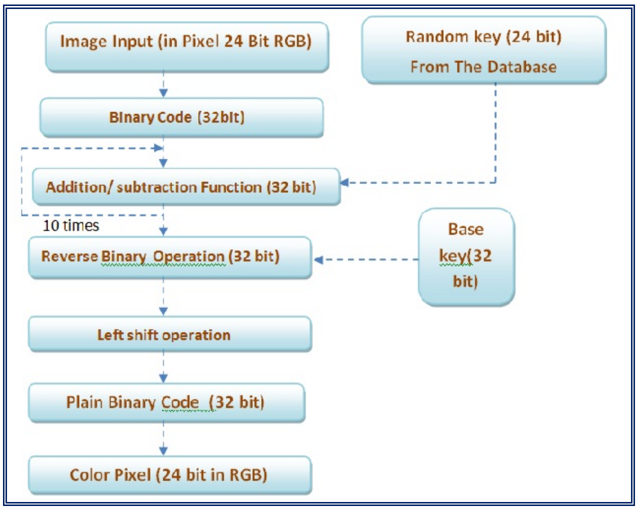
Image Input (in Pixel 24 Bit RGB)
Random key (24 bit) From The Database
Binary Code (32bit)
Addition/ subtraction Function (32 bit)
10 times
Reverse Binary Operation (32 bit)
Base key(32 bit)
Left shift operation
Plain Binary Code (32 bit)
Color Pixel (24 bit in RGB)

Figure 4. Block Diagram of SES Decryption Algorithm

V. Languages Suitable for SES

The algorithm has been implemented only in Java and it can be implemented in any language that supports Unicode system.

VI. Performance Evaluation

The most prominent feature of SES algorithm is that it is not fully dependent on the secret key. Additional secondary key is used to give an extra security edge. Moreover SES algorithm keep changing the key based on randomly chosen integer number and sequence symbol. This feature makes SES algorithm practically immune to the "Replay attacks", making it more safe and sound[1]. A chief problem in image encrypting algorithms is strong correlation between neighboring pixels due to smooth value changes in large areas of digital images[11]. SES algorithm takes this problem into account and is designed to use different primary keys to encrypt diverse pixels and hence resolving the spatial problematic issue.

Another predicament that arises in image encryption is high redundancy i.e. same color of encrypted pixels that have same color in original image. This behavior will make it easier for the cryptanalyst to decode the digital image. The high redundancy behavior is also not the concern in SES algorithm as it is taking pixel by pixel and encoding it rather than just changing colors with respect to original image. Moreover, it does different binary operations on plain message (original image) or prior cipher image making it harder to crack than traditional image encryption ciphers. The above mentioned features of SES algorithm make it securer that traditional image encrypting algorithms.

A. Timing Analysis

The SES algorithm is premeditated in such a way to accomplish prime advantage i.e. the speed of encryption and decryption of data[9]. Code optimization techniques are exercised to achieve greater encryption speed. The following table shows encryption and decryption times for SES for digital images of various sizes.

TABLE 1. Performance Analysis of SES

Input Size (Pixels)	Encryption Time (sec)	Decryption Time (sec)	Total Execution Time (sec)
300*300	2.7	2.3	5.0
500 * 500	6.5	5.5	12.0
1000 * 1000	26.0	20.0	46.0

VII. Security Analysis

Security is an important aspect for both, the encrypted objects and the encryption algorithms. Here some security issues of the SES algorithm have been discussed from the cryptography point of view in this section.

A. ***Chosen cipher text attack:*** *This attack model refers to the situation where attacker tries to deduce secret keys by studying various cipher texts and corresponding plaintexts[8]. This kind of attack has more chances of success if encryption process uses limited key values and does not change the image data too much. SES algorithm has been planned to counter such attacks. It uses two keys which are chosen randomly for different pixels; hence deduction of encryption keys will be practically impossible.*

B. Ciphertext-only attack: *In this attack model, the attacker tries to deduce the original images by studying different ciphered images[8]. If lesser portions of image is encrypted, more portions of image can be reconstructed without finding out secret key and hence it is more easier to restore real images. Here, SES encrypts every pixel of the given image and experiments show that ciphertext-only attacks are inefficient to infer the original image.*

C. ***Chosen-plaintext attack:*** *In this attack model, an attacker chooses a number of plaintexts and then interprets their respective cipher texts[9]. The attack can break the encrypted image without knowing details of encryption algorithm and secret key. But SES algorithm uses transformation and also changes the image data and pixel locations even when it is resized.*

D. ***Brute-force attack:*** *It is an attack model where attacker tries to guess security keys by doing extensive search of all possible combinations of the key[3]. It is basically hit-&-trial method and can be dangerous if a key space of encryption algorithm is limited. SES algorithm picks up a different key for every pixel from a very vast key space and hence it is quite resistant to such attacks.*

If the intruder uses a brute-force technique to break the random number, the time taken will be:

$$2*2*2*2*\ldots\ldots\ldots..16 \text{ times} = 2^{16}$$

Now the data is also associated to a sequence symbol in primary key which is 8 bits long, thus time consumption to find it will be:

$$2*2*2*2\ldots\ldots\ldots\ldots.8 \text{ times} = 2^{8}$$

Hence, total time requirement to break the primary key is:

1) *Total effort time=2^{16}*2^8= 2^{24} for one cycle*

2) *There are total 10 cycles like this and each contains the 2 different functionalities. So we must multiply by 2^{10} also. As the total cases are 2^{10}.*

3) *Total effort for the primary key = 2^{10}*2^{24}.*

VIII. Case Study

Here is an example showing the screen shots for the plaintext, cipher text and encryption process of SES algorithm applied on a 2D digital image data.

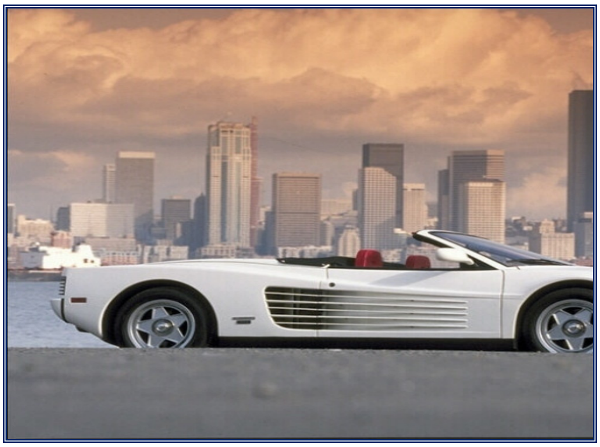

Figure 5. Plaintext read from input file

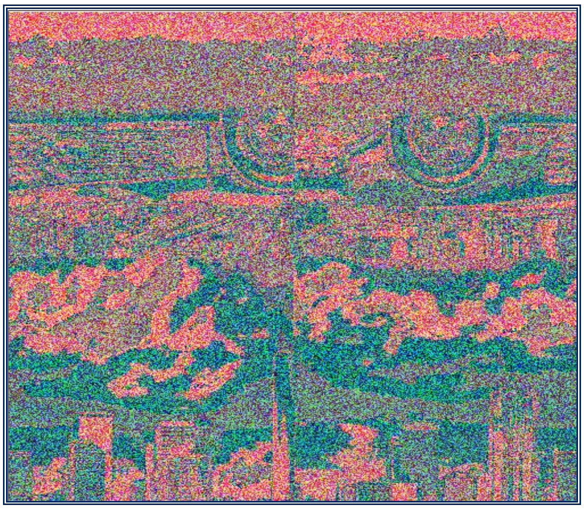

Figure 6. Cipher text obtained after applying SES

IX. Conclusion and Prospect Work

In this paper a new Stream Encryption Standard (SES) algorithm has been proposed which encodes digital image pixel by pixel. Experiments have shown that SES algorithm fully encrypts 2D digital images and original 2D images are also reconstructed without any distortion. It has been observed that only 1 out of 100 pixels is changed i.e. there is no distinct difference between original image and decrypted image. Moreover the resurrected image is exactly of the same size and with least alteration possible which is unnoticeable. The algorithm provides greater confidentiality against unauthorized attacks as well as message authentication.

Future development will include:

- Hardware execution of SES algorithm.
- Implementation of SES for speech/audio data.
- Improvement of execution time for SES.
- Realization of SES algorithm for 3D and gray scale images.
- Using compression while transferring images from one end to another and reducing memory requirements.

References

[1] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone Handbook of Applied Cryptography. New York: CRC Press, Inc., 1997.

[2] A.S. Tanenbaum, “Computer Networks”, Fourth Edition, Prentice hall, 2004.

[3] B. Schneier, Applied Cryptography : Protocols, Algorithms, and Source Code in C, John Wiley & Sons, Inc., New York, USA, 1994.

[4] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen, On the security defects of an image encryption scheme, Image and Vision Computing, p. 1371–1381, 2009.

[5] G. Prosanta, K. Akhil, A. Kushal, and K. Neeraj, “X-MODDES (eXtended Multi Operator Delimiter based Data Encryption Standard)”, ICFN, China, 2010.

[6] L. Shujun and X. Zheng, "Cryptanalysis of a chaotic image encryption method," Inst. of Image Process. Xi'an Jiaotong Univ. Shaanxi, IEEE International Symposium, Vol. 2, p. 708-711, 2002.

[7] N. Pareek, V. Patidar, K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing 24 (9), p. 926–934, 2006.

[8] P.K. Stephen and K. W. Miller, “Random Number Generators: Good ones are hard to find”, Communications of the ACM, October 1988.

[9] P.P Charles & P.L Shari, “Security in Computing: 4th edition”, Prentice-Hall, Inc.,2008.

[10] P.P. Dang, P.M. Chau, Image encryption for secure Internet multimedia applications [J].IEEE Transactions on Consumer Electronics, 46(8), p.395~403, 2000.

[11] R. Lukac, N. Konstantinous Plantaniotis, "A cost-effective encryption scheme for color images," in Science Direct real time imaging, p.454-464, 2005.

[12] W.Stallings, “Cryptography and network security principles and practice,” Fourth edition, Prentice hall, 2007.