International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

Selective Image Time Computation Chaotic with Confusion v/s 3SEMCS Encryption Algorithm in Cryptography

Manraj Singh
Department of Computer Science & Engineering,
Sri Sai Institutes of Engineering & Technology,
Manawala (Amritsar), Punjab

***Abstract*: In recent age, owing to frequent flow of digital images across the world over the transmission media, it has become essential to secure them from leakages. Image processing deals with improving the image quality. There are numerous algorithms used for encrypting the image. Chaotic and Confusion algorithm selects the portion of the image consuming a lot of time to encrypt the image results in blur shaped image which is very easy to decrypt. The objective of the work is to use the new algorithm 3SEMCS commonly named as Three Step Encryption Method for Cyber Security to improve the security level by applying three algorithms Password Hash, DES + SHA1, CAST AES algorithm results in minimum time for encryption as compared with Chaotic and Confusion algorithms. Chaotic and Confusion algorithm depicts the adjacent pixels which are attacked by statistical analysis. 3SEMCS uses very tight security so that unauthorized access cannot decrypt it and resulting image will not visible. In Computerized era, the algorithm should provide very tight security and should be encrypted and decrypted within less time. 3SEMCS algorithm shows how securely it encrypts the data at each level with text encryption enhancing the byte level of image security consuming time in seconds. At every pixel, the attacker has to find the salt key for decrypting for each level of 3SEMCS and not possible to decrypt. Chaotic system shows the salt key but 3SEMCS every salt is also encrypted depicting how fast the algorithm it is.]**

Keywords— Matlab; Selective Image Encryption; 3SEMCS; Password Hash;

I. INTRODUCTION

Selective Image Encryption is usually designed based for encrypting and compressing the data used by color images which are 3D array representation of the data streams because of numerous networks it is very difficult to secure the content of any image or private data. There are traditional approaches which perform encryption on bit stream of data to encode the data to provide huge amount of data content transmitted on the networks securing content at very high rate is now important factor in terms of transmitting the data on secure line but the requirement is to fulfill the security needs of digital images have led to the development of good encryption techniques with text encryption and for privacy protection, the only sensitive part of image is protected this sensitive selected part of an image is encrypted and can only be decrypted by registered and authorized users. Selective encryption is used to reduce the amount of data to encrypt while achieving a required level of security. The requirement is to find the time computation during Selective Image Encryption and Decryption and for enhanced privacy there is a need of text with Selective Image Encryption so as to reduce the time complexity during the Encryption/Decryption process. Selective encryption is applied into two parts: The first part is the public part which is left unencrypted and made accessible to all users and second part is the protected part and it is encrypted. Only authorized users have access to protected part. One important feature in selective encryption is to make the protected part as small as possible and there are many situation where needs the privacy of the image in minimum time. For privacy protection the only sensitive part of image is protected and this sensitive selected part of an image is encrypted and can only be decrypted by registered and authorized users. The main importance of selective encryption is to reduce the amount of data streams to encode or encrypt while achieving a required level of security.

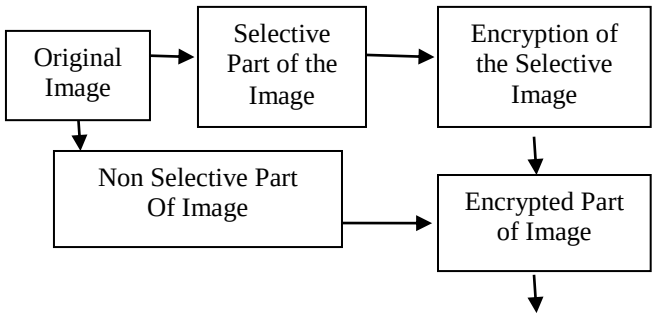

Fig 1. Process for Encryption of the Selective Image

II. RELATED WORK

Anastasios Tefas et al. [1] introduced a novel method of image authentication. They use watermark key controls to set of parameters of chaotic system for watermark generation. In this paper, the proposed method provides an additional feature of imperceptible encryption of the image owner logo in the host image. It also provides the user not only with a measure for authenticity of the test image but also with an image map that highlights the unaltered image regions when selective tampering has been made. J.M. Rodriguesa et al. [2] proposed a new approach for selective encryption in the Huffman coding of the Discrete Cosine Transform (DCT)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

coefficients using the Advanced Encryption Standard (AES). Here, Human face is partially encrypted by any image or video sequence that helps to enhance the level of security correspondingly this also allows decryption of a specific region of the image and results in a significant reduction in encrypting and decrypting processing time. Nithin MThomas et al. [3] presents a solution in the form of a novel H.264 selective encryption algorithm that encrypts sign bits of transform coefficients and motion vectors to allow secure transcoding without decryption. And after that the performance of the system is compared with I-Frame Encryption their results show that sign encryption is more secure than I-frame encryption and has a lower complexity. Ai-hong Zhu et al. [4] used encryption technology for providing security on digital image. They use chaos for the encryption of digital images and provide an improved version of encryption algorithm. The new algorithm produced nine chaotic sequences only by one secret-key, six sequences were used to scramble the position of image pixels, and the others were used to confuse and diffuse image pixels value. The performance analysis shows that the algorithm has large secret-key space, high security, fast encryption speed and strong robustness. The algorithm uses only a logistic map, but achieves a multi-chaos encryption effect. A. Kingston et al. [5] proposed a method for applying joint encryption in lossless compression technique for designed large images. They uses basic crypto-compression scheme presented is based on a cascade of Radon projection which enables fast encryption of a large amount of digital data while using standard encryption techniques such as AES, DES, 3DES, or IDEA can be applied to encrypt very small percentages of high resolution images. This proposed technique provides additional security for images based on type of standard usage. Zhang Junet al. [6] proposed a new encryption scheme for digital images based on compound Chaos algorithm is presented in this paper. The compound Chaos algorithm combines the Lorenz Chaotic system and Logistics map to generate the pseudo-random sequences then the pseudo-random sequences are used to produce the permutation matrix to encrypt the digital image. The experimental results indicate that the proposed encryption approach is valid and it can expand the secret key space and improve anti-aggressive ability. Richard E. L. Metzler et al. [7] performed selective regional encryption on nonrectangular, statistically relevant regions of image media by permutation of coefficients in the domain of a fast, shape adaptive, parametric transform in order to partially encrypt the original image. Regions were successfully segmented using a high order information analysis. A simple encryption scheme which exploits the energy compaction properties of a shape adaptive cosine transform was then applied in the transform domain. Computer simulation shows that the method is fast and statistically secure. Zhongyun Hua et al. [8] introduces a new two-dimensional Logistic-Sine map (2D-LSM). It has excellent chaotic performance and its outputs are difficult to predict. Using 2D-LSM, this paper proposes a new image encryption algorithm. Simulation results and security analysis demonstrate that the proposed algorithm is able to protect different kinds of images with a high security level.Wen Chen et al. [9] proposes a novel method named 3-D space is proposed for optical multiple-image encryption. Each input image is divided into a series of particle-like points distributed in 3-D space, and all generated particle-like points are simultaneously encrypted into a phase only mask. The proposed method may open up a novel research perspective for optical multiple-image encryption, since a 3-D-space processing strategy is developed and successfully applied. Bo Zhang et al. [10] used optical security device for XOR Encryption. This encryption technique can handle only binary signals and encrypts each pixel individually. Because images consist of pixel, we can use mask bit to encrypt it. The theoretical results are verified by computer simulation. Theoretical and computer simulation indicate that XOR encryption is a sale coding method.

III. PRESENT WORK IN MATLAB

A. Methodology

Step1. Browse an Image.

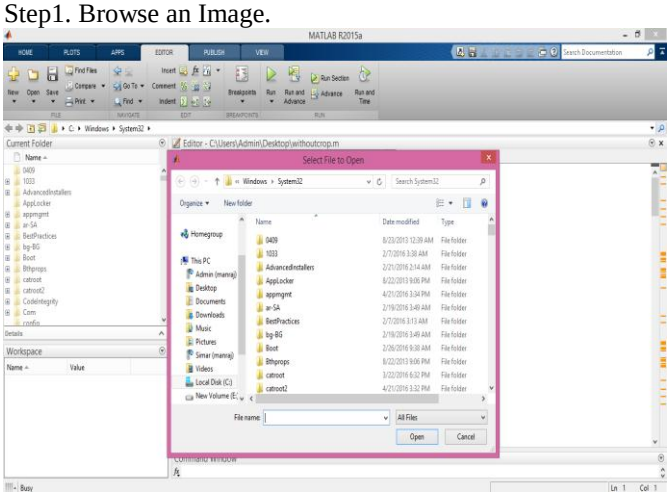

Fig 2. Browse an Image

Step2. Choose the Sensitive part of the Selected Image

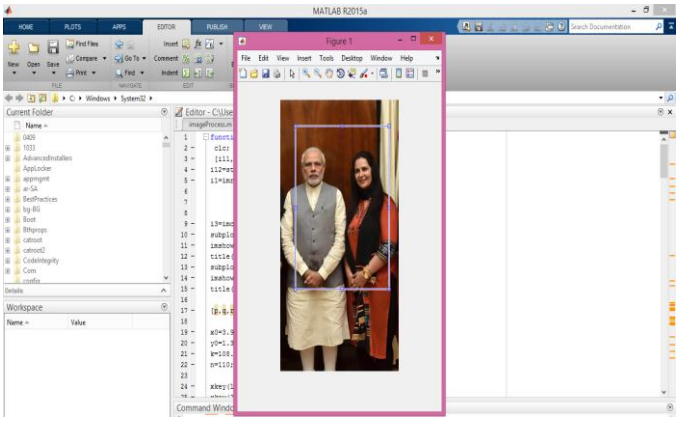

Fig 3. Select the Portion of Image

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

Step3. Apply Chaotic with Confusion Algorithm

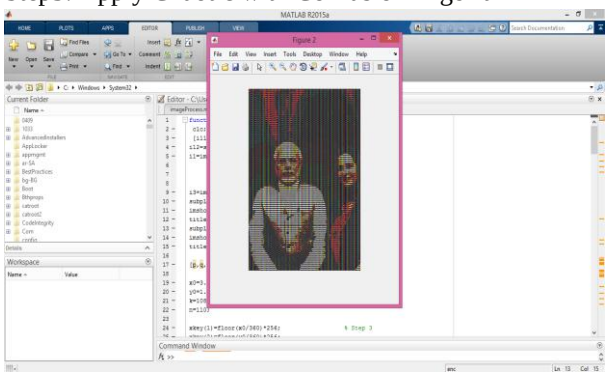

Fig 4. Selected Image After Encryption

Step4. Computing Time for Encryption

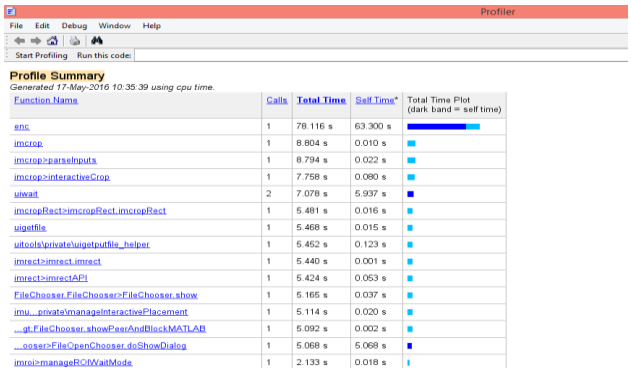

Fig 5. Time for Encryption is more than 30 seconds

Hence Chaotic and confusion algorithms takes a lot of time in encrypting the data image and result having blur shape.

IV. PROPOSED WORK IN .NET

A METHODOLOGY FOR CHAOTIC and Confusion Algorithm

1. Select the Portion of the Image

2. .Divide Image into two Parts. Apply the Chaotic and Confusion Algorithm on first part of an Image.

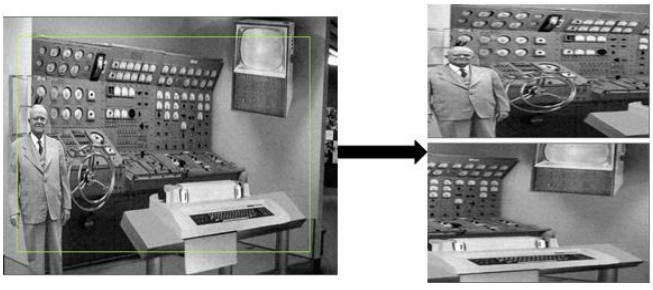

Fig6. Showing the Selected Portion and Divided into Two Parts

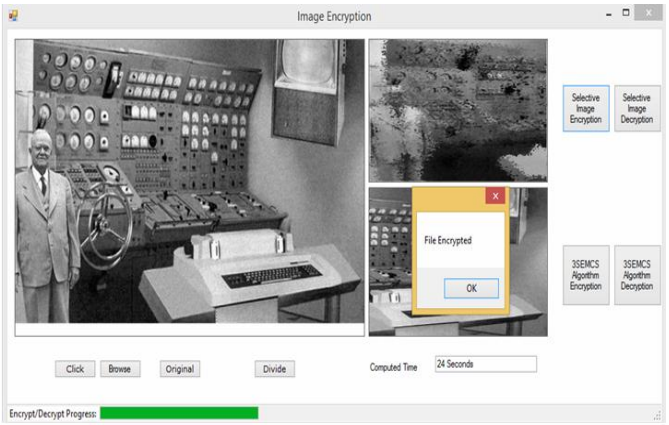

Fig7. Showing Chaotic with Confusion Algorithm takes 24 seconds to encrypt the Image

3. Compute the Encryption Time for Selective Image Encryption

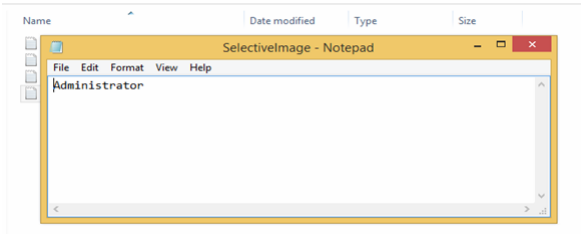

Fig8. Showing Salt Key text Saved in the Notepad File

B METHODOLOGY FOR 3SEMCS

4. Selecting the Second Image Part.

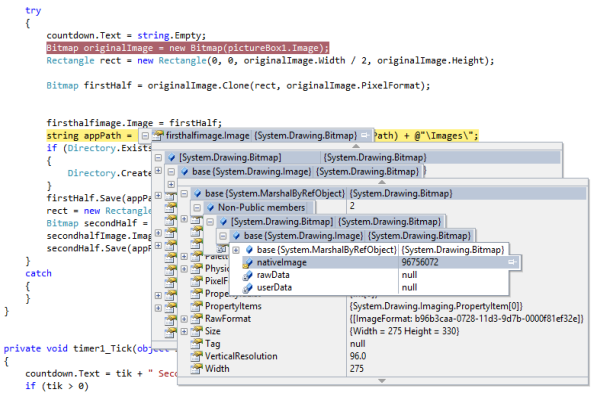

Fig9. Showing Selecting Second Part of Image

5. Apply 3SEMCS Algorithm on the second half image. First Apply the Password Hash Algorithm

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

```
class PasswordHash
{
    // The following constants may be changed without breaking existing hashes.
    public const int SALT_BYTE_SIZE = 24;
    public const int HASH_BYTE_SIZE = 24;
    public const int PBKDF2_ITERATIONS = 1000;

    public const int ITERATION_INDEX = 0;
    public const int SALT_INDEX = 1;
    public const int PBKDF2_INDEX = 2;

    /// <summary>
    /// Creates a salted PBKDF2 hash of the password.
    /// </summary>
    /// <param name="password">The password to hash.</param>
    /// <returns>The hash of the password.</returns>
    public string CreateHash(string password)
    {

        // Generate a random salt
        RNGCryptoServiceProvider csprng = new RNGCryptoServiceProvider();
        byte[] salt = new byte[SALT_BYTE_SIZE];
        csprng.GetBytes(salt);

        // Hash the password and encode the parameters
        byte[] hash = PBKDF2(password, salt, PBKDF2_ITERATIONS, HASH_BYTE_SIZE);
        return PBKDF2_ITERATIONS + ":" +
            Convert.ToBase64String(salt) + ":" +
            Convert.ToBase64String(hash);
    }
```

Fig10. Showing Password hash Algorithm

6. Apply DES + SHA1 Algorithm

```
    EncryptFile(pathString + "\\PasswordHash.txt", pathString + "\\DES.txt", cshash.hashcode);

//Calculation of the specified byte group designated area hash value

SHA1 ha = new SHA1Managed();

byte[] hb = ha.ComputeHash(keyByteArray);

//The encryption key array

byte[] sKey = new byte[8];

//Encryption variables

byte[] sIV = new byte[8];

for (int i = 0; i < 8; i++)

    sKey[i] = hb[i];

for (int i = 8; i < 16; i++)

    sIV[i - 8] = hb[i];

//Access to the encryption key

des.Key = sKey;

//Set encryption initialization vector

des.IV = sIV;
```

Fig11. Showing DES + SHA1 Algorithm

7. Apply CAST AES 256 Algorithm with Rijndael Managed Algorithm

```
string passtext = cshash.hashcode;
string passPhrase = "AGARAMUDHALA";
string saltV = "EZHUTHELLAM";
string hashstring = "SHA1";
int Iterations = 3;
string initVect = "@1B2c3D4e5F6g7H8";
int keysize = 256;
string functionReturnValue = null;
// Convert strings into byte arrays.
// Let us assume that strings only contain ASCII codes.
// If strings include Unicode characters, use Unicode, UTF7, or UTF8
// encoding.
byte[] initVectorBytes = null;
initVectorBytes = Encoding.ASCII.GetBytes(initVect);
byte[] saltValueBytes = null;
saltValueBytes = Encoding.ASCII.GetBytes(saltV);

// Convert our plaintext into a byte array.
// Let us assume that plaintext contains UTF8-encoded characters.
byte[] plainTextBytes = null;
plainTextBytes = Encoding.UTF8.GetBytes(passtext);
// First, we must create a password, from which the key will be derived.
// This password will be generated from the specified passphrase and
// salt value. The password will be created using the specified hash
// algorithm. Password creation can be done in several iterations.
PasswordDeriveBytes password = default(PasswordDeriveBytes);
password = new PasswordDeriveBytes(passPhrase, saltValueBytes, hashstring, Iterations);
// Use the password to generate pseudo-random bytes for the encryption
// key. Specify the size of the key in bytes (instead of bits).

keyBytes = password.GetBytes(keysize / 8);
// Create uninitialized Rijndael encryption object.
RijndaelManaged symmetricKey = default(RijndaelManaged);
```

Fig12. Showing CAST AES 256 Algorithm

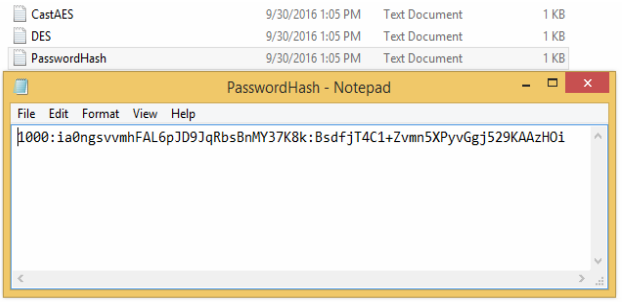

Fig13. Showing Password Hash for Text

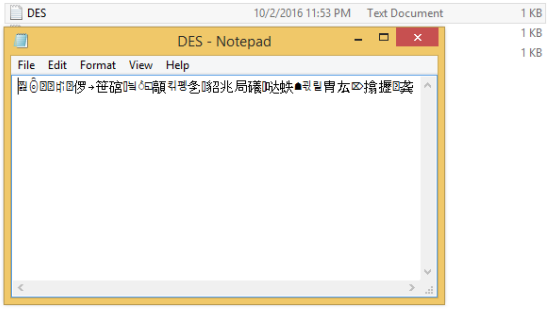

Fig14. Showing Image Data in Text File

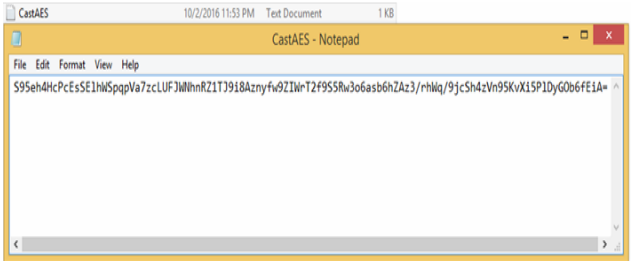

Fig15. Showing CAST AES 256 in Text File

8. Compute the Overall Encryption Time.

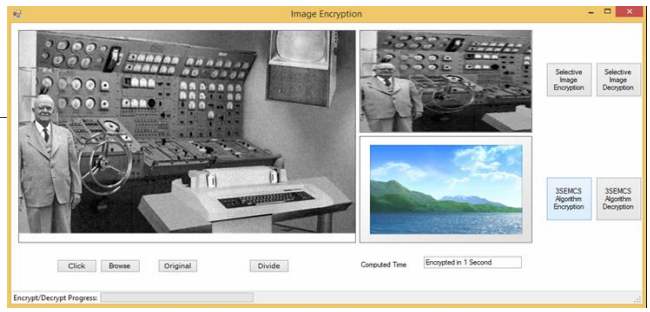

Fig16. Showing just 1 sec to encrypt the Image

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

9. Compute the Encryption Time for Selective Image Encryption.

Fig17. Showing Overall Time Computation

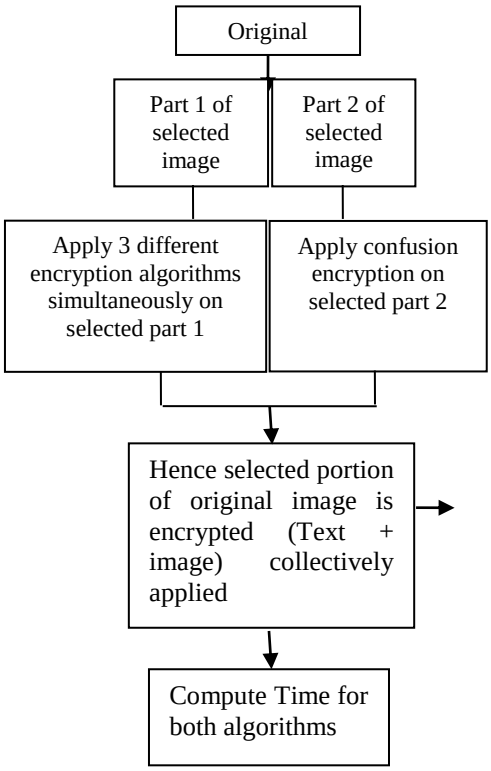

Fig18. Flowchart showing the Proposed Technique

B. PERFORMANCE ANALYSIS

This paper has designed and implemented the proposed technique in .NET Visual Studio.

Chaotic with Confusion Algorithm depicts the following encryption time.

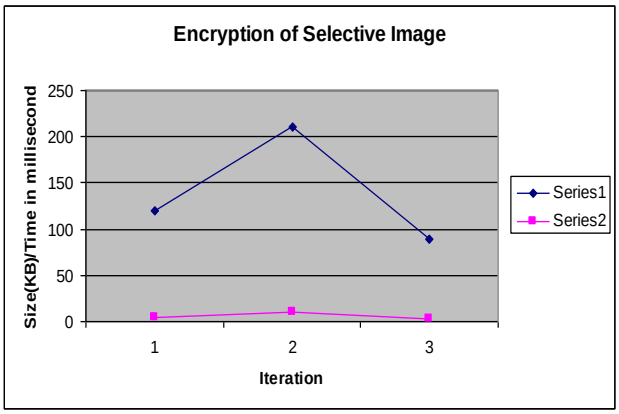

Fig 25. Encryption time for Selective part of Image

3SEMCS Algorithm depicts the following encryption time

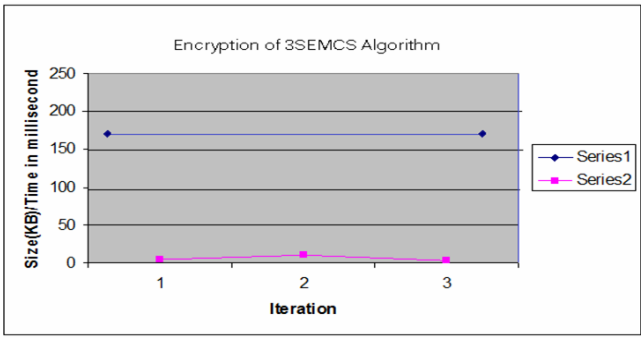

Fig 26 . Encryption time for 3SEMCS

V. CONCLUSION AND FUTURE WORK

The future scope concerns with Privacy of Highly Data Stream Images which usually have to encrypt and compress the size of the content in minimum time so that it will provide higher level of security on the transmission line. In Future Video Sizes will be Encrypted and Decrypted using 3SEMCS by using frame sizes. However 3SEMCS encrypts the whole Data Stream into the Text File, so it is difficult to decrypt without the key. It will reduce the cost effectiveness of the algorithm and provide securable system encrypted in Minimum Time.

REFERENCES

[1] *Anastasios **Tefas** and Ioannis Pitas.* Image Authentication using chaotic mixing systems. IEEE International Symposium on Circuits and Systems, Geneva, Switzerland, 2000.
[2] J.M. Rodriguesa, W Puecha and A.G. Borsb. Selective Encryption of Human Skin in JPEG Images. IEEE, 2006.
[3] Nithin MThomas, Damien Lefol, David R Bull, David Redmill. A NOVEL SECURE H.264 TRANSCODER USING SELECTIVE ENCRYPTION.IEEE,2007.
[4] Ai-hongZhu and Lian Li. Improving for Chaotic Image Encryption Algorithm Based on Logistic Map. 2nd Conference on Environmental Science and Information Application Technology,2010.
[5] *A. Kingston, S. Colosimo, P. Campisi and F. Autrusseau.* Lossless Image Compression and Selective Encryption using a Discrete Radon Transform.IEEE, 2007.
[6] Zhang Jun, Li Jinping and Wang Luqian. A New Compound Chaos Encryption Algorithm for Digital Images. International Forum on Information Technology and Applications, 2010.
[7] Richard E. L. Metzler and Sos S. Agaian. Selective Region Encryption Using a Fast Shape Adaptive Transform.IEEE, 2014.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 01, January-2017

[8] Zhongyun Hua, Yicong Zhou, Chi-Man Pun, C. L. Philip. Image encryption using 2D Logistic-Sine chaotic map. IEEE International Conference on Systems, Man, and Cybernetics, 2014.
[9] Wen Chen. Optical Multiple-Image Encryption Using Three-Dimensional Space. IEEE Photonics Journal. IEEE, April 2016.
[10] Bo Zhang, MTE Kahn. Simulation of optical XOR encryption using MATLAB.IEEE, 2004.