Hybrid Video Encryption System with Integrating W7 and A5 Framework

Mr. Mithilesh Dewangan[1], Mr. Deepak Shrivastava [2]

[1] *M.Tech. Scholar, CSE Department, DIMAT, Raipur*
mithilesh.dewangan@gmail.com,

[2] *Asst.Professor, CSE Department, DIMAT, Raipur*
dshrivastava76@gmail.com

Abstract— Images play a pivotal role in several applications like remote sensing, biomedical, videoconferencing. Interests in digital image processing methods stems from the following principal application areas: improvement of pictorials information for human interpretation; and processing of image data for storage and transmission for machine perception. Image Encryption means changing convert the image into unreadable format. This can be done by modifying the images pixels in terms of its (place, Value) in order to protect the information.

Image encryption plays a significant role in the field of information hiding. Generally there are two levels of security for digital image encryption: low level and high level. In low level security encryption, the encrypted image has a degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. The proposed Encryption approach reduces the data and compresses the image with much more efficiency than the conventional method. The study in the work has proved that the B – Frame is most efficient and most secured frame among all the frames. It uses less storage capacity, and formation of cipher secures the image with proper process of Encryption and Decryption.

Keywords—Bio Medical Video Conferencing; Remote Sensing; Digital Image Processing, Image Encryption, Decryption.

I. INTRODUCTION

Images play a pivotal role in several applications like remote sensing, biomedical, videoconferencing. Interests in digital image processing methods stems from the following principal application areas: improvement of pictorials information for human interpretation; and processing of image data for storage and transmission for machine perception

Image Encryption means changing convert the image into unreadable format. This can be done by modifying the images pixels in terms of its (place, Value) in order to protect the information. There can be many technique to encrypt image which involve may be key mapping or hiding of fusion of image ,but basically the image is changed at pixels level i.e. value of pixels or their position in original array.

Image encryption plays a significant role in the field of information hiding. Generally there are two levels of security for digital image encryption: low level and high level. In low level security encryption, the encrypted image has a degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewer. In the high level security, the content is completely scrambled and the image appears as random noise. In such case, the visual characteristic of the image is not understandable to the viewers. The proposed techniques of image encryption in this thesis can be categorised under high-level security encryption. The security of a cipher should only rely on the decryptions key D_{kd}, since an adversary can recover the plaintext from the observed ciphertext once he/she gets D_{kd}.

Figure 1.1 shows a block diagram for encryption/decryption of a cipher.

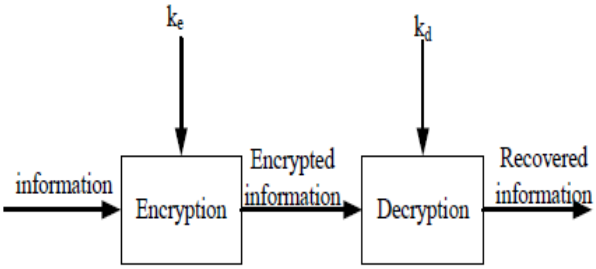

Fig 1.1: Encryption/Decryption of cipher

Classical encryption algorithms are sensitive to keys, while chaotic maps are sensitive to initial condition and parameters. Cryptographic algorithms shuffle and diffuse data by rounds of encryption, while chaotic maps spread

the initial regions over the entire phase space via iterations. Permutations are important mathematical building block for symmetric encryption systems in general, and block ciphers in particular. Permutation is a bijective map whose domains and range are the same. Permutation ciphers based on chaos have been proposed.

a. Chaotic Mapping

Basically it scrambles the images following a particular algorithm and reversing it can find the base image. It can be seen from the following: The N × N Image is divided diagonally into two maps(Left and Right).Left map means The Image is first transformed into a line of pixels and then shuffled using algorithm,After that again it is converted to N × Nimage(Encrypted).

b. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) is a symmetric cryptosystem that proposed for content encryption by Rijmen and Daemen in 1999, furthermore known as Rijndal algorithm, however a few scientists made functional use of this algorithm for image encryption likewise with a few changes in key generation and other requirements.

II. Problem Identification

Digital images, accounting for 70% of the information transmitted on the Internet, are important parts of network exchanges. However, the image information, which is different from text message, has larger scale of data, higher redundancy and stronger correlation between pixels. Statistical analysis of encrypted images provides much information about the
security of a cipher with reference to statistical attacks that could be launched against the cipher. There are two important methods of statistical analysis of encrypted images. The first is histogram analysis and the second is the adjacent pixel correlation analysis.

a) Issues in the field of Image Encryption

1) Encrypted images of MASK do not reveal any texture of original image.
2) Histograms of encrypted images of MASK exhibit uniform distribution of pixel gray levels over the entire range. This indicates effectiveness of MASK encryption.
3) Adjacent pixel correlation in the encrypted images of MASK is very low. This shows that the pixels in the MASK encrypted images are statistically independent.
4) Mean value plots of encrypted images of MASK show that the mean value of pixels across the encrypted image is uniform compared to that of the original image. This also shows MASK encryption is effective.
5) Key sensitivity analysis of encrypted image of MASK indicates that one bit change in secret key brings 33% change in the encrypted image.
6) The encryption speed measurement shows that MASK encryption is eight times faster than AES. Thus MASK is efficient in converting plaintext data and images into ciphertext data and cipher images.
7) The average encryption quality is more in MASK compared to AES.Encryption quality of MASK is 967.72 and that of AES is 956.82 for animage of size 512× 512 pixels.
8) Unlike text messages, the multimedia information including image data has some special characteristics like high capacity, redundancy and high correlation among pixels. In some cases image applications require to satisfy their own needs like real time transmission and processing.

b) Knight Tour Problem

Knight's Tour Problem (KTP) is one of the oldest problems in chess and computer algorithms. The puzzle is all about moving the Knight throughout the chessboard of dimension (8 x 8) in 63 moves covering each square only single time. If starting from a square, the knight approaches the same place as beginning after traversing through entire chessboard, the tour is called closed otherwise open knight's tour.

III. Related Work

Komal D Patel and SonalBelani (2011) have worked on "Image Encryption Using Different Techniques" and in present times, the protection of multimediadata was becoming very important. The protection of this multimedia data can be done with encryption. There were so many different techniques should be used to protect confidential image data from unauthorized access. In this paper, we survey on existing work which was used different techniques for image encryption and we also give general introduction about cryptography.

Shuai Wang et al. (2013) have worked on "Design and Analysis of Fast Image Encryption Algorithm based on Multiple Chaotic Systems in Real-time Security Car" and inthis paper takes intelligent security car as the research background, aiming to find a image encryption algorithm to realize the car in the image secure transmission of wireless transmission network based on open protocols, with good safety and high real-time. this passage was based on the analysis of the existing encryption algorithms of traditional and new image, select the digital image encryption technology based on chaotic system, And put forward a Multiple chaotic image encryption method which was fit for this project, After analysis and test, the algorithm satisfies the requirements of safety and real-time.

Xiping He and Qionghua Zhang (2008) have worked on "Image Encryption Based on Chaotic Modulation of Wavelet Coefficients" and in this paperwereaimed at the image encryption scheme applicable to JPEG2000 codec. Firstly, two chaotic maps were suggested and their statistic characteristics were also analysed. Secondly, to accomplish a controllable visual effect of encrypted image, a visual quality control model was presented, and on the basis of which, a chaotic image encryption scheme was constructed by chaotically modulating the randomly selected approximate coefficients at the coarsest level in wavelet domain. Then, the security and efficiency of the algorithm were analysed. Finally, the experiment results illustrate that the proposed algorithms were credible, secure, efficient, and practical for JPSEC.

Weihai Li and Nenghai Yu (2009) have worked on "A Robust Chaos-Based Image Encryption Scheme" and A DCT domain image encryption scheme based on chaotic shuffling table was proposed, in which the shuffling tables were generated by several Logistic maps. This scheme was robust to normal image processing, such as noising, smoothing, compressing, and even print-scan processing. In this scheme, key space was easy to be adjusted by choosing the number of Logistic maps. The encrypted image was still highly compressible since shuffling operation was confined in DCT equal-frequency coefficients. What was more, a random number, called nonce, was introduced to initialize initial values of Logistic maps, which ensures that the proposed scheme can resist chosen-plain-text cryptanalysis.

Narendra K Pareek (2012) has worked on "Design and Analysis of a Novel DigitalImage EncryptionSceme" and in this paper, a new image encryption scheme using a secret key of 144-bits was proposed. In thesubstitution process of the scheme, image was divided into blocks and subsequently into color components.Each color component was modified by performing bitwise operation which depends on secret key as wellas a few most significant bits of its previous and next color component. Three rounds were taken tocomplete substitution process.

Dr.A.Sampath et al. (2011) have worked on "Enhancement and Analysis of Chaotic Image Encryption Algorithms" and the focus of this paper was to improve the level of security and secrecy provided by the chaoticmap based image encryption.An encryption algorithm based on the Logistic and the Henonmaps was proposed. The algorithm uses chaotic iteration to generate the encryption keys, andthen carries out the XOR and cyclic shift operations on the plain text to change the values ofimage pixels. Chaotic Map Lattice based image encryption algorithm suggested by Pisarchik was also examined which was based on Logistic map alone.

Smita R. Chunamari and D. G. Borse (2013) have worked on "Secure Schematic Model for Verifying Encrypted Image using Invariant Hash Function" and in post globalization era of computer networks and communication, image and video play a significance role; rather the fashion of text based systems will be replaced by the image based system. The associated threats and challenges related to image security and its authentication was an active research issues. In order to ensure a full proof security mechanism for image the notion of message authentication code for data authentication and notion of encryption for preserving confidentiality need to be combined. In this paper a complete frame work of crypto-system has been proposed.

IV. METHODOLOGY

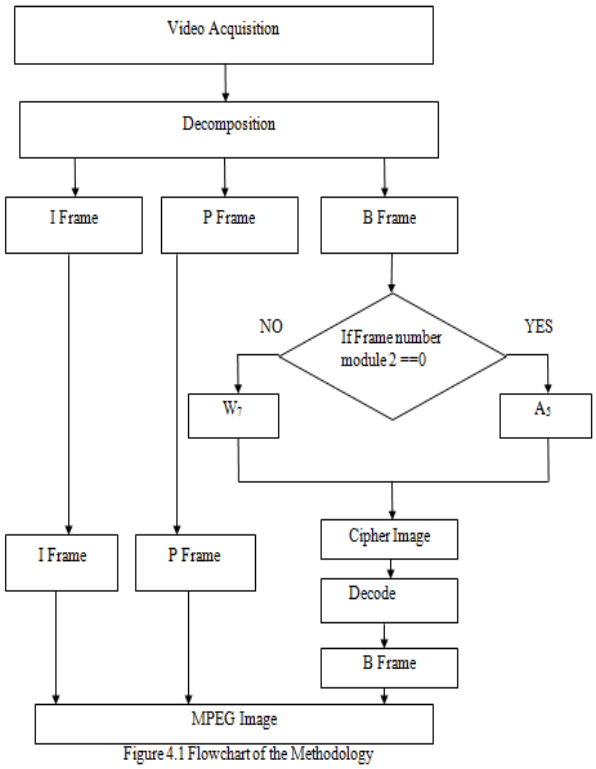

Figure 4.1 Flowchart of the Methodology

To perform the experiment, we will need the MATLAB Tool for Simulation.

Methodology in Detail

Step 1:- Video Acquisition

- Video acquisition is the process of converting an analog video signal such as that produced by a video camera or DVD Player to digital video.
- It is the process of sampling the signals that measure real world physical condition and convert the resulting samples into digital numeric value that can be manipulated by a computer.

Step 2:- Decomposition

- Decomposition is also known as Factoring, which is breaking a complex problem or system into parts that are easier to conceive, understand, program and maintain.
- Once the phase congruency map of an image has been constructed we know the feature structure of the image. As was mentioned above, the standard way of compressing this feature structure is to apply a threshold, thus reducing a rich image representation to a simple binary structure. However, thresholding is course, highly subjective, and in the end eliminates much of the important information in the image.
- Some other method of compressing the feature information needs to be considered, and some way of extracting the non-feature information, or the *smooth map* of the image, needs to be developed. In the absence of noise, the feature map and the smooth map should comprise the whole image.
- When noise is present, there will be a third component to any image signal, and one that is independent of the other two. This approach was developed in his thesis and used to develop an image compression technique that works very effectively on images with fine feature detail, where the standard algorithms like JPEG fail to maintain image fidelity.

Step 3:- I - Frame

- An I - Frame (Inline Frame) is an HTML document embedded inside another HTML document on a website. The I - Frame HTML element is often used to insert content from another source, such as an advertisement, into a Web page.
- It means Intra Frame, which is a video compression method used by MPEG Standards.
- In a motion sequence, individual frames of pictures are grouped together and played back, so that the viewer register the video – spatial motion.

Step 4:- B - Frame.

- It is a Shortcut for Bidirectional Frame, a video compression method used by the MPEG standard. In a motion sequence, individual frames of pictures are grouped together (called a *group of pictures*, or *GOP*) and played back so that the viewer registers the videos spatial motion.
- It is a leading provider of collections and accounts receivable management software for collection agencies.
- As the name suggests, B-frames rely on the frames preceding and following them. B-frames contain only the data that have changed from the preceding frame or are different from the data in the very next frame.

Step 5: P – Frame.

- It is a shortcut to the Productive frame, which is a video compression method used by the MPEG standards.
- P – Frame follows I – Frame and contains only the data that have changed from the preceding I – frame.
- Because of this, P-frames depend on the I-frames to fill in most of the data.

Step 6:- Check for the value of Frame Number module, i.e. if it is zero or not and wait for the formation of the cipher image.

- If the value of Frame number module is zero, then A5, otherwise if the frame number module has the value not equal to zero , then W7.
- Now, after this the Cipher image is formed, which is an image used as an algorithm for performing encryption or decryption that is a series of well defined image that can be followed as a procedure.
- The cipher image is a intermediate form of the image formed , which is used to decrypt or decode here

Step – 7 - Decode the image and obtain MPEG Image.

- Now the image is decrypted from the cipher to the original form in which it has to be obtained.
- There is a key to the cipher which helps the image to get decoded and changes into the standard MPEG Format.
- At last an MPEG Image is obtained, whose efficiency is high , security is high and redundancy is less.

RESULTS AND DISCUSSIONS

Based upon the steps discussed in the Methodology, the graphical user interface is designed in MATLAB, which makes the task easier.

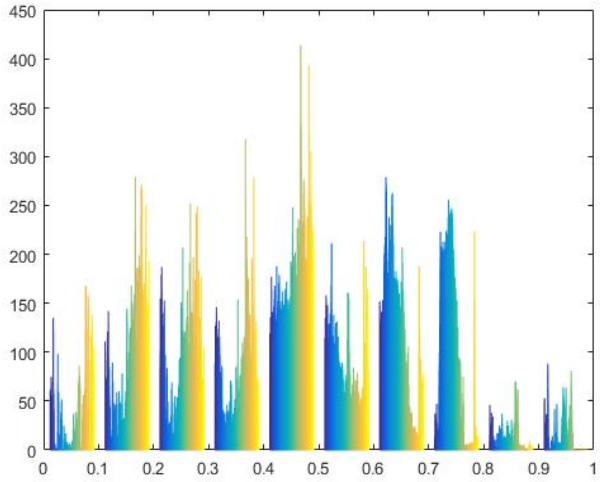

Fig 1- Histogram graphs of encryption algorithm

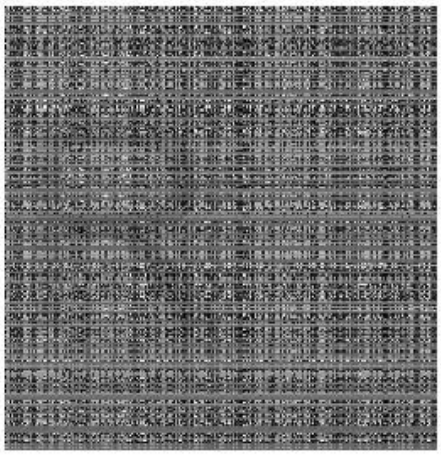

FIG 2 – THE ENCRYPTED FRAMES

CONCLUSION AND FUTURE WORK

The proposed Encryption approach reduces the data and compresses the image with much more efficiency than the conventional method. The study in the work has proved that the B – Frame is most efficient and most secured frame among all the frames. It uses less storage capacity, and formation of cipher secures the image with proper process of Encryption and Decryption. In this approach, a successfully efficient implementation of A5/1 and W7 scheme for digital image encryption was done.

As a future scope, a simplified MPEG codec can be easily developed for the process of embedding the perceptual

video cipher to overcome the drawback. Also, the degradation in the visual quality is completely dependent on the amplitudes of the intra-DC coefficients.

REFERENCES

[1] H.Zhu, C. Zhao andX. Zhang,"A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem", Image Communication, vol.28,**(2013)**, pp.670-680.

[2] Y. Zhang, D. Xiao, Y. Shu and J. Li, "A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations", Image Communication, vol. 28, **(2013)**, pp. 292-300.

[3] S. Behnia, A. Akhavan, A. Akhshani and A. Samsudin. "Image encryption based on the Jacobian elliptic maps", Journal of Systems and Software, vol. 86, **(2013)**, pp. 2429-2438.

[4] C.-H. Lin, T.-H. Chen and C.-S. Wu, "A batch image encryption scheme based on chaining random grids", Scientia Iranica, vol. 20, **(2013)**, pp. 670-681.

[5] A. Bakhshandeh and Z. Eslami. "An authenticated image encryption scheme based on chaotic maps and memory cellular automata", Optics and Lasers in Engineering, vol. 51, **(2013)**, pp. 665-673.

[6] A. A. Abd El-Latif, L. Li, N. Wang, Q. Han and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces", Signal Processing, vol. 93, **(2013)**, pp. 2986-3000.

[7] F. Li and J. Xu, "Image encryption algorithm based on Hash function and multiple chaotic systems", Computer Engineering and Design, vol. 31, **(2010)**, pp. 141-144.

[8] Y. Zhang, L. Wu and S. Wang, "Improved ant colony algorithm based on membership cloud models", Computer Engineering and Applications, vol. 47, **(2011)**, pp. 201-205.

[9] T. Gao and Z. Chen, "A new encryption algorithm based on hyper-chaos", Phys. Lett, vol. 372, **(2008)**, pp. 394-400.

[10] C. He, L. Chen and Z. Wang, "Chaotic image scrambling algorithm based on magic cube", Computer System Applications, vol. 19, **(2010)**, pp. 50-53.

[11] W. Hou and C. Wu, "Image encryption and sharing based on arnold transform", Journal of Computer Applications, vol. 31, **(2011)**, pp. 2681-2686.

[12] J. Liu, C. Zhu and Y. Wang. "Image scrambling effect evaluation method based on position correlation", Computer Engineering, vol. 36, **(2010)**, pp. 208-210.