RESEARCH ARTICLE OPEN ACCESS

ROBUST VIDEO DATA HIDING USING FLEXIBLE MACROBLOCK ORDERING

K. Geetha Rani[1], B. Banu Priya[2], S. Gayathri[3], J. Jetlish Stephani[4]

[1]Assistant Professor, Department of Computer Science and Engineering,

Loyola Institute of Technology, Chennai.

[2,3,4]UG students, Department of Computer Science and Engineering,

Loyola Institute of Technology, Chennai.

----------**********----------

Abstract:

Data hiding technique can be used to embed a secret message into a compressed video. This new video data hiding method makes use of erasure correction capability of Repeat Accumulatecodes and superiority of Data Hiding. Flexible Macroblock used for message hiding and unhiding. This method withstands frame drop and insert attacks. The proposed solutions are analyzed in terms of message extraction accuracy, excessive bit rate and quality distraction. RSA algorithm is used for key generation. The cover video is divided into number of frames in which the data can be hidden into blocks of frame. The video which contains secret data is called stegno video. The extraction of data is done using FMO technique.

Keywords —**frames, accuracy, flexible macroblock ordering, extraction.**

----------**********----------

I. INTRODUCTION

Stegnography is the basis of data hiding. Stegnography is the practice of hiding a file, message, image or video within another file, message, image or video. The advantage of stegnography over cryptography is that intended secret message does not attract attention to itself as an object of scrutiny. Cryptography is the practice of protecting te contents of a message alone whereas stegnography is concerned with cincealing the fact that a secret message is being sent as well as concealing the contents of the message.

The security problem in various data transfering and via internet can be addressed by cryptography and stegnography. Stegnography is the method to avoid data being significant effective in preventing others from attempting the decryption while the information is hidden in the host object as the secret data element.

Cryptography always cause the other data to decryption for its encryption format. But stegnography place an important role to hiding the secret information and make the video as invisible. By using stegnography the information from the people can be safely moved to the other people, mainly this process is for security.

Most of the people communicate and share the private information over internet. When the secret information shared, it should have secure technique that blocks the data from intruders and hackers. However, we are using the efficient algorithm to detect the secret data from the hackers. The algorithm contains the high embedding efficiency to reduce suspicion of finding the hidden data.

In this paper, we are using RSA algorithm to generate keys. The Rivest-Shamir-Adleman (RSA) algorithm is the most popular and secure public key encryption method. The fact is there is no effiecient way to factor very large as (100-200) digit numbers. So we are using the encryption key as (e,n) and the decryption key as (d,n). The user of RSA creates and then publishes the product of two large prime

numbers, along with the auxiliary value, as their public key. RSA invloves both private and public key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted with public key can only be decrypted with the private key.

In existing system, the main idea is to hide data or file into a cover video using DCT-based BCH error correcting method. This method converts the video into frames which then divides each frame into Y, U and V components. These frames are converted into YCbCr colour space. This conversion is to remove the correlation between the red, green and blue colours. Here used a method BCH (7,4,1) codes where the message has been encrypted using a secret key and produced encoded message. 2D-DCT is applied on each plane individually. The extraction of hidden message is done by isolating the stego video into frames. This can be done by taking D_k digits of DCT coefficient, except DC coefficient. In the proposed system, we use a technique called FMO to embed the data and file into the cover video. The RSA algorithm is used for key generation to encrypt the secret data or file to encoded message. The Flexible Macroblock Ordering is used to divide an image into regions called slices. Each slice contains a sequence of macroblocks and can be decoded independently of other slices. These macroblock can normally be processed from left to right, beginning at the top. Usually a frame can have single slice or multiple slices. If there is an error in a slice, it propogate within the slice. FMO enhances this by allowing macroblocks to be grouped and sent in any direction and order. All video codecs allow Region of Interest coding, in which specific macroblocks are targeted to receive more or less quality. FMO's primary benefit when combined with RoI coding is the ability to prevent errors in one region from propogating into another region. FMO allows inter prediction for immediate neighbouring slices, in the same group, effectively making a contiguous region nearly act like single slice, where slice groups are shaped into Region of Interest. It helps to improve efficiency over simple slices. FMO should only be used where packet losses are common and expected. This method is introduced inorder to reduce the distortion and breaking of frames and to provide efficiency.

II. EXPERIMENTALWORKS:

After the data and video are selected, the data now to be hidden into the cover video. Before that the data should be changed into encoded data through encryption using RSA algorithm. To hide, the Flexible Macroblock Ordering (FMO) technique is used.

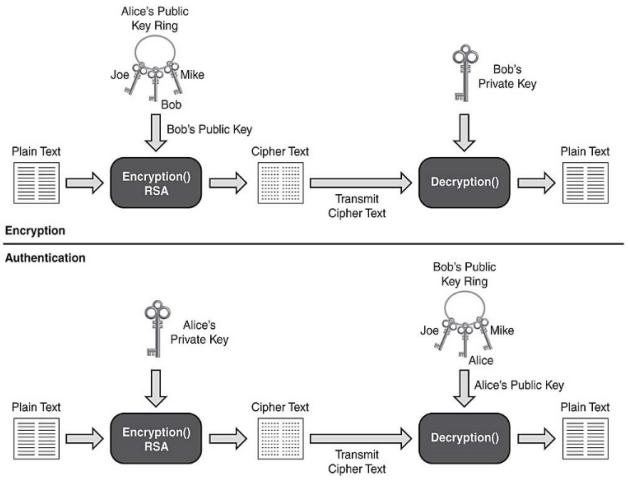
A. *RSA*:

RSA is traditional public key cryptography. It has atmost significant advance in history of cryptography. This algorithm uses two keys – a public and a private key. It can also be said as asymmetric since parties are not equal. This public key scheme is neither more secure than private key (security depends on the key size for both) , nor do they replace private key schemes (they are too slow to do so). It is called asymmetric because those who encrypt messages or verify signatures cannot decrypt message or create signatures. This two-key algorithm uses public key, which may be known by anybody and can be used to encrypt messages and verify signatures.

RSA is developed by Rivest, Shamir and Adleman of MIT in 1977. It is based on exponentiation in a finite (Galois) field over integers modulo a prime. (exponentiation takes $O((\log n)^3)$ operations). There are three approaches to attacking RSA: (i) brute force key search (infeasible given size of numbers), (ii) mathematical attacks (based on difficulty of computing $\Phi(N)$, by factoring modulus N), (iii) timing attacks (on running of decryption).

The RSA algorithm provides confidentiality, integrity, authenticity and non-reputability of electronic communication and data storage. RSA derives the security from the difficulty of factoring large integers that are the product of two large prime numbers. Multiplying these two numbers is easy, but determining the original prime number from the total factoring is considered infeasible due to the time it would take even using today's super computer.

Figure (a)ENCRYPTION AND AUTHENTICATION



The public and private key generation algorithm is most complex part of RSA cryptography. Two prime numbers p and q are generated using Rabin-Miller primilarity test algorithm. A modulus n is calculated by multiplying p and q. This number is used by both the public and private keys and provides the link between them. Its length usually expressed in bits is called key length.

Figure (a) represents the diagramatical representation of encryption and decryption of RSA algorithm using public and private keys respectively.

The public key consists of modulus n and a public exponent e which is normally set at 65537, as its prime number that is not too large. The private key consists of modulus n and the private exponent d, which is calculated using the extended Euclidean algorithm to find the multiplicative inverse with respect to the totient of n.

Figure (b)DIFFERENT KEY SPECIFICATION

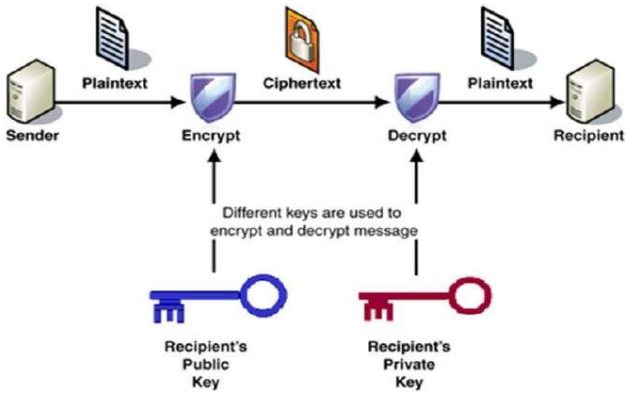


Figure (b) represents combination of the encryption and decryption technique of figure (a) in a single representation.

ALGORITHM[21]:

1. Choose two different large random prime numbers p and q.
2. Calculate n = p x q

   n is the modulus for the public key and the private key.
3. Calculate the totient:

   $\Phi(n) = (p-1)(q-1)$
4. Choose an integer e such that $1 < e < \Phi(n)$, and e is coprime to $\Phi(n)$.

   i.e., e and $\Phi(n)$ share no factors other than 1 ;

   $$\gcd(e, \Phi(n)) = 1$$

   e is released as public key exponent.
5. Compute d to satisfy the congruence relation.

   $$d\,e \equiv 1 \pmod{\Phi(n)}$$

   d is kept as the private key exponent.
6. Encryption :

   $$c \equiv m^e \pmod{n}$$
7. Decryption :

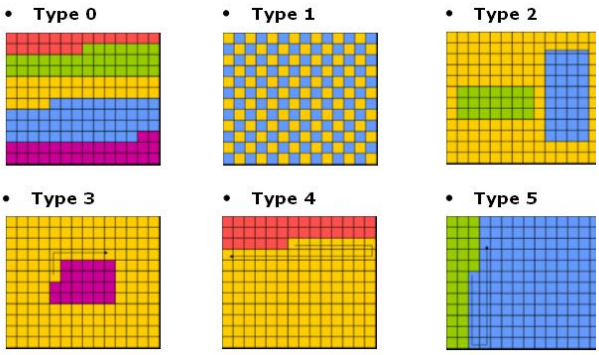
   $$m \equiv c^d \pmod{n}$$

B. FLEXIBILE MACROBLOCK ORDERING:

Flexible Macroblock Ordering is one of the most interesting resilient feature within the H.264/AVC , which is a new standard for digital video compression. Using FMO, it is no longer required that slices consists of neighbouring macroblocks. Each macroblock can be assigned freely to a certain slice group using a macroblock allocation map (MBAmap). To prevent complex allocation schemes, the number of slice groups is limited to eight gor each picture.

FMO consists of seven different types, labeled Type 0 to Type 6. Type 6 is the most random one and allows full flexibility to the user. The other ones all contain a certain pattern. These patterns can be exploited when storing and transmitting the MBAmap.

Figure (c) TYPES OF FMO



FMO type 0 uses runlengths which are repeated to fill the frame. Therefore only those runlengths have to be known to rebuild the MBAmap on the decoder side.

FMO type 1, also known as scattered slices, uses a function, which is known to both the encoder and decoder, to spread the macroblocks. The more slice groups used, the more each macroblock will be surrounded by macroblocks from different slice groups.

FMO type 2, is used to mark rectangular areas, so called Region of Interest, inside a frame. MBAmaps can be stored using the top left and bottom right coordinates of those rectangles.

Types 3 to 5 are dynamic ones and let the slice groups grow and shrink over the different pictures in a cyclic way. Only the grow rate, the direction and the position in the cycle have to be known.

APPLICATION ON USING FMO TECHNIQUE:

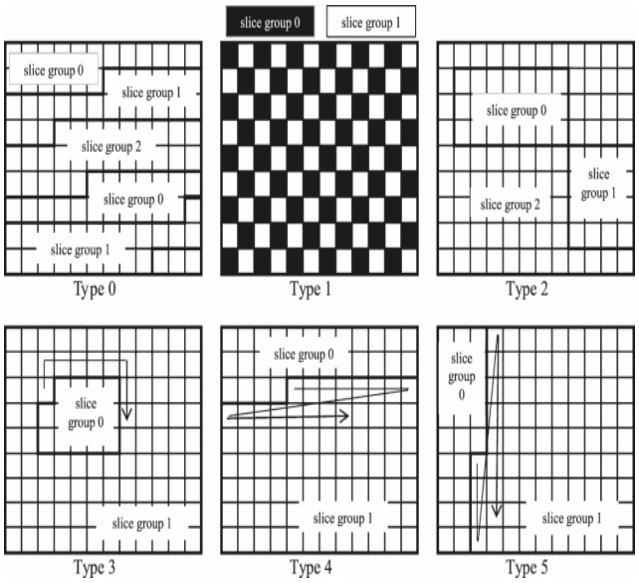
Broad cast over cable, satellite, cable modem, DSL, terrestrial etc. Interactive or serial storage on optical and magnetic devices, DVD etc. Video-on-demand or multimedia streaming services over ISDN, cable modem, DSL, LAN, wireless network etc. Multimedia messaging services over ISDN, DSL, Ethernet, LAN wireless or mobile networks etc.

It significantly enhances the robustness to data loses by managing the spatial relationship between the regions that are used in each slice. MPEG-4 moves away from traditional view of video as a sequence of rectangular frames. Instead collection of video objects. A video object is a flexible entity that a user can access and manipulate.

A depth overview is given of the internals of the FMO experiments are presented that demonstrate the benefits of FMO as an error resilience tools in case of packet loss over IP networks. The flexibility of FMO covers with a certain overhead or cost. A quantitative assessment of this cost is presented for a number of scenario, FMO besides for pure error resilience also be used for other purposes.

The H.264/AVC standard provides several new error resilient features to enable the reliable transmission of compressed video signals over lossy packet networks, flexible macro block is one of the most interesting resilient features within the H.264/AVC standard unlike former standards in which slices were constructed out of consecutive master scan macro blocks, FMO suggest new slices composed in a mixed-up fashion.

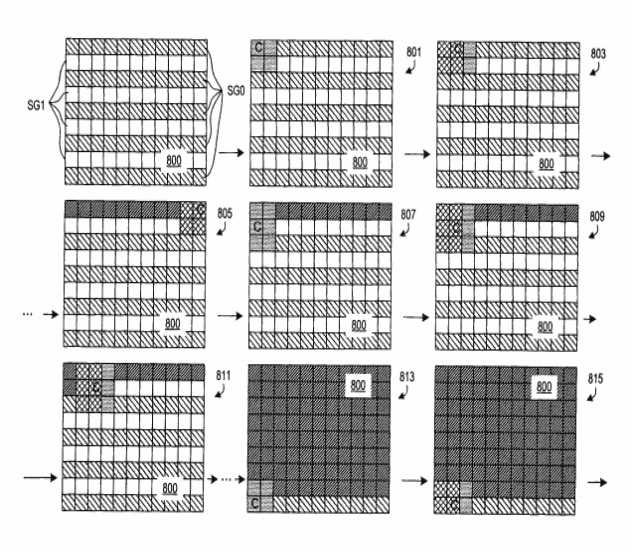
Figure (d) SLICE GROUPS



A video object is an arbitrarily shaped area of scene that may exist for an arbitrary length of time. Definition encompasses traditional view of rectangular frames too. Macro block may be kept whole or divide horizontally into two sub blocks of size 16*8 or 8*16. Divided into4 sub blocks (8*8) and hence 4 sub block may be divided once more into a 2 or 4 smaller blocks.

H.264/AVC is a new standard for digital video compression jointly developed by ITU-TIS video coding export group and ISO/2EC's moving picture experts group (MPEG). Reside the numerous tools for efficient video coding the H.264/AVC specification defines some errors resilience tools, one of them is Flexible macro block ordering (FMO).

Figure (e) SECTION OF SLICES



H.264/AVC specifies seven types of FMO. The standard defines also an explicit FMO type which allows explicity assignment of each MB within the former to any available slice groups. Therefore, a new FMO technique can be used and integrated into H.264/AVC without violating the standard.

The new ECW ordering results in effective error scattering which maximizes number of correctly received macroblocks located around corrupted macroblocks leading to better error concealment.

Performance evaluations demonstrate that the proposed explicit FMO approach outperformance all the FMO types. Both subjective and objective visual quantity comparative study has been also carried out in validate the proposed approach.

III. CONCLUSION AND FUTURE ENHANCEMENT:

Video criteria such as motion alleviation, GOP size and bitrate were recommended as guidelines to select appropriate technique for information hiding, and future research directions were suggested. In addition, we aim at proposing new information hiding methods or consolidating

the existing ones for actual application purposes such as video compression, motion tracking, etc. We also aim for exploring new information hiding opportunities in the latest video compression standard.

The method not only detects the stego frames precisely, but also estimates the gain factor and original frame. To this end, noise reduction by soft thresholding and also block matching were used for cover estimation. As the results confirm, the proposed method has excellent performance in detecting the stego frames while it estimates the gain factor and the hidden message with high precision.

The FMO was used to allocate macroblocks to slice groups according to the content of the message. Comparisons with existing work revealed the effectiveness of the proposed solutions in terms of message payload, video distortion and excessive overhead. Future work includes examining the robustness of the proposed work against channel bit errors, packet losses and existing digital video stego analysis methods.

REFERENCES

[1] R. J. Mstafa and K. M. Elleithy, "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes," Multimedia Tools and Applications, pp. 1-23, 2015.

[2] R. J. Mstafa and K. M. Elleithy, "A highly secure video Steganography using Hamming code (7, 4)," in Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island, 2014, pp. 1-6.

[3] C. Chin-Chen, T. D. Kieu, and C. Yung-Chen, "A High Payload Steganographic Scheme Based on (7, 4) Hamming Code for Digital Images," in Electronic Commerce and Security, 2008 International Symposium on, 2008, pp. 16-21.

[4] L. Guangjie, L. Weiwei, D. Yuewei, and L. Shiguo, "An Adaptive Matrix Embedding for Image Steganography," in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on, 2011, pp. 642-646.

[5] W. Jyun-Jie, C. Houshou, L. Chi-Yuan, and Y. Ting-Ya, "An embedding strategy for large payload using convolutional embedding codes," in ITS Telecommunications (ITST), 2012 12th International Conference on, 2012, pp. 365-369.

[6] R. J. Mstafa and K. M. Elleithy, "A New Video Steganography Algorithm Based on the Multiple Object Tracking and Hamming Codes," in 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA), 2015, pp. 335-340.

[7] R. Zhang, V. Sachnev, and H. Kim, "Fast BCH Syndrome Coding for Steganography," in Information Hiding. vol. 5806, S. Katzenbeisser and A.-R. Sadeghi, Eds., ed: Springer Berlin Heidelberg, 2009, pp. 48-58.

[8] R. Zhang, V. Sachnev, M. B. Botnan, H. J. Kim, and J. Heo, "An efficient embedder for BCH coding for Steganography," Information Theory, IEEE Transactions on, vol. 58, pp. 7272-7279, 2012.

[9] Y. Liu, Z. Li, X. Ma, and J. Liu, "A Robust Data Hiding Algorithm for H. 264/AVC Video Streams," Journal of Systems and Software, 2013.

[10] I. Diop, S. M. Farss, K. Tall, P. A. Fall, M. L. Diouf, and A. K. Diop, "Adaptive steganography scheme based on LDPC codes," in 2014 16th International Conference on Advanced Communication Technology (ICACT), 2014, pp. 162-166.

[11] A. K. Jain, Fundamentals of digital image processing: Prentice-Hall, Inc., 1989.

[12] W. B. Pennebaker and J. L. Mitchell, JPEG: Still image data compression standard: Springer Science & Business Media, 1992.

[13] Y. Hoyoung, J. Jaehwan, J. Jihyuck, and P. In-Cheol, "Area-Efficient Multimode Encoding Architecture for Long BCH Codes," Circuits and Systems II: Express Briefs, IEEE Transactions on, vol. 60, pp. 872-876, 2013.

[14] R. J. Mstafa and K. M. Elleithy, "A high payload video Steganography algorithm in DWT domain based on BCH codes (15, 11)," in WirelessTelecommunications Symposium (WTS), 2015, 2015, pp. 1-8.

[15] R. J. Mstafa and K. M. Elleithy, "An Efficient Video Steganography Algorithm Based on BCH Codes," in American Society for EngineeringEducation (ASEE Zone 1), 2015 Zone 1 Conference, Boston, 2015, p. 10.

[16] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," Multimedia Tools and Applications, pp. 1-27, 2015/05/24 2015.

[17] S. Hu and U. KinTak, "A Novel Video Steganography based on Nonuniform Rectangular Partition," in Computational Science andEngineering (CSE), 2011 IEEE 14th International Conference on, 2011, pp. 57-61.

[18] K. Patel, K. K. Rora, K. Singh, and S. Verma, "Lazy Wavelet Transform Based Steganography in Video," in Communication Systems andNetwork Technologies (CSNT), 2013 International Conference on, 2013, pp. 497-500.

[19] M. A. Alavianmehr, M. Rezaei, M. S. Helfroush, and A. Tashk, "A lossless data hiding scheme on video raw data robust against H.264/AVC compression," in Computer and Knowledge Engineering (ICCKE), 2012 2nd International eConference on, 2012, pp. 194-198.

[20] R. J. Mstafa and K. M. Elleithy, "A novel video Steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes," in Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island, 2015, pp. 1-7.

[21] William, Stalling, (2014), "Cryptography and network security-Principles and practice", Sixth Edition, Pearson Education, Inc.