International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 8, Number 1 (2016), pp. 35-41
© International Research Publication House
http://www.irphouse.com

Secure Data Transmission with Enhancement of Reversible Watermarking

[1]Asma Mohammed Shareef
M. Tech Student, Dept. of Computer Science & Technology,
Mahaveer Institute of Science & Technology, Bandlaguda, TS, India.

[2]B. Sasidhar
Professor, Dept. of Computer Science & Technology,
Mahaveer Institute of Science &Technology, Bandlaguda, TS, India.

[3]M. Sreenivas Reddy
Assistant Professor, Dept. of Computer Science & Technology,
Mahaveer Institute of Science &Technology, Bandlaguda, TS, India.

Abstract

This paper proposes a secure data transfer among people. Watermarking is the kind of activity which prevents the revealing of interactive messages. Video files are usually a set of pictures. Thus most of the conferred techniques on pictures and audio will be applied to video files too. The good benefits of video are the massive quantity of knowledge that may be hidden within and also they have no problematic fact that it's a moving stream of image. During this design, a replacement technique uses the motion vector, to cover the information within the framing objects is developed. Moreover, to enhance the protection of the information, it is encrypted by using the DES formula then hidden. The information is hidden within the horizontal and also the vertical elements of the framing objects.

Keywords: Data hiding, encrypted domain, H.264/AVC, code word substituting.

INTRODUCTION

The users are increased on the web which one among the foremost necessary factors of data technology and communication has been the safety of data. Cryptography was created as a way for securing the secrecy of communication and plenty of completely different strategies are developed to inscribe and decode information so as to stay the message secret. Inappropriately, it's generally not adequate for the important matter of a message to remain secret, it should even be necessary that the existence of the message remains secret. The technique to implement is named Watermarking. Watermarking[3] constraints on keeping, wherever it keeps the important lines of a message secret in cryptography and it moves from cryptography within the sense on the important matter of a message secret in cryptography, watermarking constraint on keeping the existence of a message secret Watermarking and cryptography square measure each way in which to safeguard data from unwanted parties. Once the presence of hidden data is discovered or maybe suspected, the aim watermarking part is defeated. The strength of watermarking will therefore be amplified by adding it with cryptography**.**

LITERATURE SURVEY:

In the year 2014, SamanIftikhar, M. Kamran, and Zahid Anwarhas had developed the “RRW—A Robust and Reversible Watermarking Technique for Relational Data” [15][17], in which they had said that the advancement in information technology is playing an increasing role in the use of information systems comprising relational databases. These databases are used effectively in collaborative environments for information extraction; consequently, they are vulnerable to security threats concerning ownership rights and data tampering. Watermarking is advocated to enforce ownership rights over shared relational data and for providing a means for tackling data tampering. When ownership rights are enforced using watermarking, the underlying data undergoes certain modifications as a result of which, the data quality gets compromised. Reversible watermarking is employed to ensure data quality along-with data recovery. However, such techniques are usually not robust against malicious attacks and do not provide any mechanism to selectively watermark a particular attribute by taking into account its role in knowledge discovery. Therefore, reversible watermarking is required that ensures; (i) watermark encoding and decoding by accounting for the role of all the features in knowledge discovery; and, (ii) original data recovery in the presence of active malicious attacks. In this paper, a robust and semi-blind reversible watermarking (RRW) technique for numerical relational data has been proposed that addresses the above objectives. Experimental studies prove the effectiveness of RRW against malicious attacks and show that the proposed technique outperforms existing ones.

D.M.Thodi and J. J. Rodriguez had proposed another approach of new reversible (lossless) watermarking algorithm for digital images by prediction-error expansion method [12]. Being reversible, the algorithm enables the recovery of the original host information upon the extraction of the embedded information. The proposed technique exploits the inherent correlation among the adjacent pixels in an image region using a predictor. The information bits are embedded into the prediction errors, which enables us to embed a large payload while keeping the distortion low. A histogram shift at the encoder enables the decoder to identify the embedded location.

Y.-C. Liu, Y.-T Ma, H.-S Zhang, D.-Y Li and G S. Chen. has worked on a method for trust management in cloud computing i.e data coloring based on cloud watermarking using the computing environment[4].With virtualization technology, cloud computing offers diverse services (such as virtual computing, virtual storage, virtual bandwidth, etc.) for the public by means of multi-tenancy mode. Although users are enjoying the capabilities of super-computing and mass storage supplied by cloud computing, cloud security still remains as a hot spot problem, which is in essence the trust management between data owners and storage service providers. In this paper, we propose a data coloring method based on cloud watermarking to recognize and ensure mutual reputations. The experimental results show that the robustness of reverse cloud generator can guarantee users0 embedded social reputation identifications. Hence, our work provides a reference solution to the critical problem of cloud security.

In the watermarking schemes evaluation F.A.Petticolas demonstrated which has allowed him for the tremendous ability to access and redistribute digital multimedia contents. In such a context, protecting the ownership and controlling the copies of digital data have become very important. Watermarking technique is used to impose ownership rights over shared relational data and for providing a means for tackling data tampering. When ownership rights are imposed using watermarking, the underlying data undergoes certain modifications; as a result of which, the data quality gets compromised. The main aim is to maintain the ownership of Relational Database and also minimizing distortion in the watermarked content. Therefore, reversible watermarking is required that ensures watermark encoding and decoding by accounting for the role of all the features in knowledge discovery and original data recovery.

Later on by studing the above aspects the activity method like least vital bit (LSB) replacement, is finished in special domain, whereas remodel domain methods; hide knowledge in another domain like ripple domain.

Least significant bit (LSB) is that the simplest variety of Stenography. LSB relies on inserting knowledge within the least vital little bit of pixels that cause a small modification on the quilt image that's not noticeable to human eye. Since this technique are often cracked simply, to attacks which is more susceptible.

Hence there is a chance for attacker to know the information as the secret key used for cryptography of compressed image and information concealing is same. And also the original video can be retrieved from the changed video when extracting or removing the information hidden within the image.

PROPOSED SYSTEM

Since LSB technique has intense effects on the applied math info of image like bar graph. Attackers may well be awake to a hidden communication by simply checking the bar graph of a picture. An honest answer to eliminate this defect was LSB matching. LSB-Matching was an excellent success in Watermarking strategies and lots of others get ideas from it. By using this methodology, the data concealing in video is performed in two important ways: bit stream-level and data-level. During this paper model, we have to propose a brand new block-based selective in a tendency embedding sort information concealing Framework. By suggesting easy rules in to the frame markers are applied, we have a direction to introduce bound level of strength against frame drop, repeat and insert attacks.

With these we may overcome the limitations of existing system by increasing the protection, security, dimensions of hold on information .We will hide quite one bit.

ARCHITECTURAL DIAGRAM

The below figures shows the architectural diagram for the proposed system i.e., Secure Data Transfers among users with the help of Reversible Watermarking. It shows how the messages are hidden in the videos and transferred among others

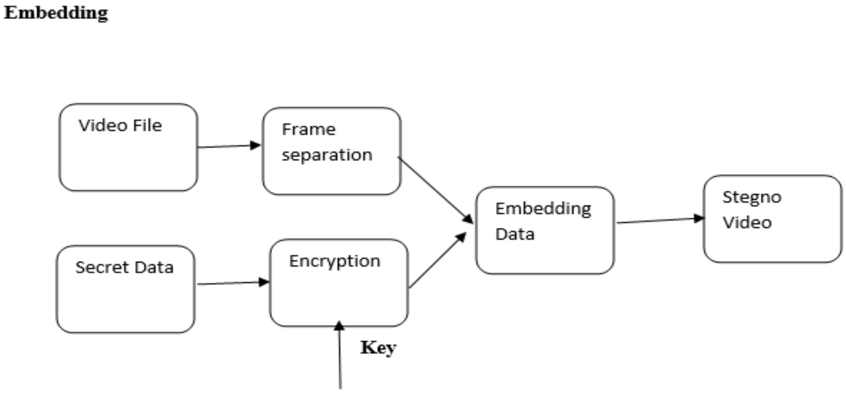

Fig 1: Block Diagram for embedding the info into the videos

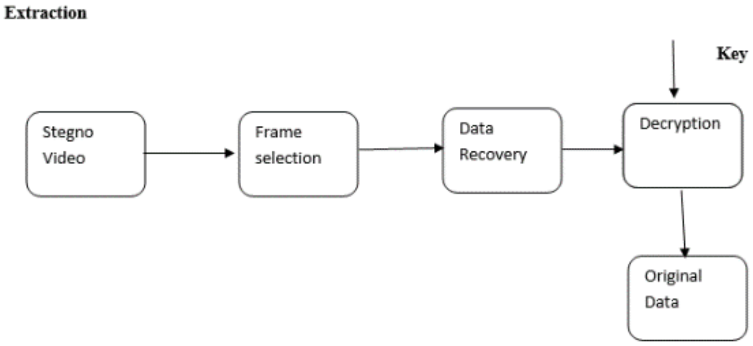

Fig 2: Block Diagram for extracting the messages from the videos

PHASES:

a) Video compression
b) Encryption
c) Embedding
d) Extracting

Video Compression

Video compression uses fashionable writing techniques to cut back redundancy in video knowledge. Video compression usually operates on square-shaped teams of neighboring pixels, usually referred to as macro blocks. These picture element teams or blocks of pixels area unit compared from one frame to consecutive and also the video compression code sends solely the variations inside those blocks. In areas of video with additional motion, the compression should inscribe, to stay up with these pixels are larger variety of additional knowledge that area unit dynamical.

Encryption

Encryption is that the conversion of knowledge into a type, referred to as a cipher text that can't be simply understood by unauthorized individuals. Original message is being hidden inside a carrier specified the changes thus occurred within the carrier don't seem to be noticeable. data the knowledge the data} regarding the user outlined information, the decoding non-public key wont to cipher the text and also the average time of the frame format is given. The encoding of the text is finished by victimizations the DES customary algorithmic rule since the key size is larger for the DES.

Extraction of original data

Decoding is that the method of changing encrypted knowledge back to its original type, thus it will be understood. Once the user inputs the right key that's used at the decoding method, this can extract the first message that's encrypted and embedded.

CONCLUSION

In this paper, there is a tendency to propose and investigate the information concealing methodology exploitation the motion vector technique for the moving objects. Within the existing works the information is hidden at intervals the still photos wherever because it can result in the image distortion. By embedding the information within the moving objects the standard of the video is raised. The compressed video is employed for the information transmission since it will hold giant volume of the information. The compression technique is mostly evaluated within the vertical and horizontal part pixels specified the information is embedding. The PSNR rate is calculated to output that the point of frame is transmitted with no loss or distortion. As a result, the motion vector technique is found because the higher resolution since it hides the information within the moving objects instead of within the still photos. The cryptography enhances the protection of the information being transmitted.

REFERENCES

[1] W. J. Lu, A. Varna, and M. Wu, “Secure video processing: Problems and challenges,” in Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859.

[2] B. Zhao, W. D. Kou, and H. Li, “Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol,” Inf. Sci., vol. 180, no. 23, pp. 4672–4684, 2010.

[3] W. Puech, M. Chaumont, and O. Strauss, “A reversible data hiding method for encrypted images,” Proc. SPIE, vol. 6819, pp. 68191E-1–68191E-9, Jan. 2008.

[4] Y.-C. Liu, Y.-T. Ma, H.-S. Zhang, D.-Y. Li, and G.-S. Chen, “A method for trust management in cloud computing: Data coloring by cloud watermarking,” Int. J. Autom. Comput, vol. 8, no. 3, pp. 280–285, 2011.

[5] X. P. Zhang, “Reversible data hiding in encrypted image,” IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[6] W. Hong, T. S. Chen, and H. Y. Wu, “An improved reversible data hiding in encrypted images using side match,” IEEE Signal Process. Lett., vol. 19, no. 4, pp. 199–202, Apr. 2012.

[7] X. P. Zhang, “Separable reversible data hiding in encrypted image,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[8] K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[9] A. V. Subramanyam, S. Emmanuel, and M. S. Kankanhalli, “Robust watermarking of compressed and encrypted JPEG2000 images,” IEEE Trans. Multimedia, vol. 14, no. 3, pp. 703–716, Jun. 2012.

[10] S. G. Lian, Z. X. Liu, and Z. Ren, “Commutative encryption and watermarking in video compression,” IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007.

[11] G. Gupta and J. Pieprzyk, “Reversible and blind database watermarking using difference expansion,” in Proc. 1st Int. Conf. Forensic Appl. Tech. Telecommun., Inf., Multimedia Workshop, 2008, p. 24.

[12] X. Li, B. Yang, and T. Zeng, “Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection,” IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524– 3533, Dec. 2011.

[13] S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang, “Secure advanced video coding based on selective encryption algorithms,” IEEE Trans. Consumer Electron., vol. 52, no. 2, pp. 621–629, May 2006.

[14] D. W. Xu and R. D. Wang, “Watermarking in H.264/AVC compressed domain using Exp-Golomb code words mapping,” Opt. Eng., vol. 50, no. 9, p. 097402, 2011.

[15] Saman Iftikhar, M. Kamran, and Zahid Anwar “ RRW—A Robust and Reversible Watermarking Technique for relational data” IEEE Transactions on knowledge and data engineering, vol. 27, no. 4, april 2015

[16] D. W. Xu, R. D. Wang, and J. C. Wang, "Prediction mode modulated data-hiding algorithm for H.264/AVC," J. Real-Time Image Process., vol. 7, no. 4, pp. 205–214, 2012.

[17] K. Jawad and A. Khan, "Genetic algorithm and difference expansion based reversible watermarking for relational databases," J. Syst. Softw., vol. 86, no. 11, pp. 2742–2753, 2013.