Different Level Multi Media Content Delivery System based on Advance Watermark Algorithms

S. P. Sri Ragavi
Master Of Computer Application
Kongu Engineering College
Perundurai, Erode

L. Rahunathan
Assistant Professor
Department of Computer Application
Kongu Engineering College
Perundurai, Erode

***Abstract*— Digital watermarking of multimedia content is more commonly known. Particularly image watermarking—a derivative of Steganography is an age-old practice allowing covert transmission of messages from one party to another party. In existing system a major drawback of these techniques is that they modify the data to a very large extent which often results in the loss of data quality. In proposed system a reversible data hiding in encrypted images. In the first phase, a data holder encrypts the original uncompressed image using an encryption key. Then, a data-hider may restore the least significant bits of the encrypted image using a data-hiding key. With an encrypted image contain excess data, when a receiver has the data-hiding key, can remove the excess data then does not know the image data. If the receiver has both the data-hiding key and the encryption key, easily can extract the all data and retrieve the original content without any problem.**

Index Terms — Steganography, Least significant bits, Water marking encoding, decoding, recovery,

I. INTRODUCTION

Information security is designed to protect the computer system data with the hateful intention. Confidential, Integrity and Availability are refer as CIA triad of information security. This triad is commonly termed the parkerian hexad, which includes control, confidentiality, authenticity, availability, and integrity. Sensitive information must be kept – it cannot be changed, altered or transferred without permission. For example, a message could be modified during transmission by someone intercepting it before it reaches the intended recipient. Good cryptography tools can help mitigate this security threat.

The original image is encrypted date using an encryption key and the excess data are enclosed with the encrypted image using the date hiding key. The encrypted image contain the excess or additional data, if the receiver has only the data-hiding key, then they can extract the additional data thus he does not know the image the encryption content. If they have only the encryption key, can decrypt the received data to get an image alike to the original one, but cannot extract the enclosed additional data. If the receiver has both the data hiding key and the encryption key They can extract the additional data and recovery the original image without any problem when the number of additional data is too large.

In RRW (Robust Reversible Watermark), the knowledge of common information for every candidate element is also employed to compute the watermark information. Then, it is ensure that the data quality will not be affected. So, Robust Reversible Watermark provides a robust solution for data recovery that is reversible and flexible against heavy attacks.

The proposed system implements all the existing system methodologies. In addition, the RGB color image is taken for image encryption. During image encryption pseudo-random bits are X-or with image pixel bits as in existing system. During reverse process, either the original image or text alone can be retrieved by the receiver. In addition, text input data is perturbed such that random characters are embeds inside the original text. Moreover, the text data is encrypted using Triple DES encryption and then hide in to the encrypted image.

This paper is organized as follows as (1) data preprocessing phase, (2) watermark encoding phase, (3) attacker channel, (4) watermark decoding phase and (5) data recovery phase.

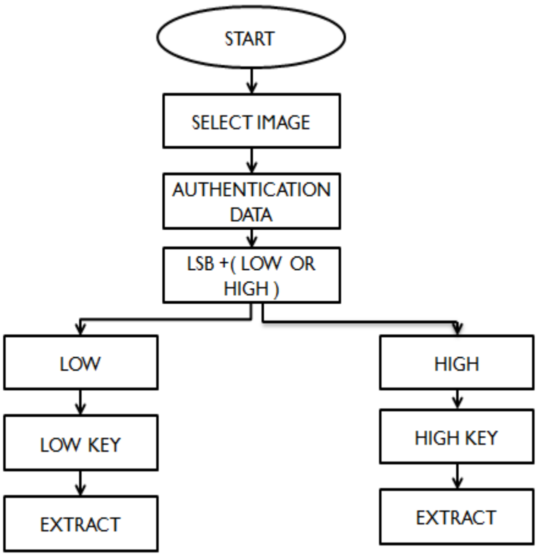


Fig no 1: Work flow content delivery system

II. RELATED WORKS

Nassir Memon and Ping Wah Wong is described as digital watermarking recently proposed for the copy protection and copy deterrence for multimedia content. In copy protection and copy deterrence, a content owner insert the watermarking into the copy of content before sold to a buyer. If the buyer sells unauthorized copies of the watermarked content, these can be traced by the unlawful original seller using the watermarking detection algorithm. One of the problems in that the original buyer whose watermark has been found on unauthorized copy can claim that the unauthorized copy was created by the original seller. We proposed that in this paper are interactive with buyer-seller does not get to know the exact watermarked. In cases Of seller send an unauthorized copy, the seller can identify the buyer in the authorized copy. This prevents the buyer from claiming that an authorized copy may have originated from the seller.

Mina Deng, Tiziano Bianchi, et al, describes as Buyer-seller watermarking protocols integrate watermarking techniques with cryptography, for official document protection, privacy tracing, and privacy protection. In this paper, we propose an efficient buyer seller watermarking protocol based on homomorphism public-key cryptosystem and composite signal representation in the encrypted domain. A freshly proposed composite signal representation allows us to decrease both the computational overhead and the large communication and width which are due to the use of homomorphic public-key encryption schemes. Both difficulty analysis and simulation results prove the efficiency of the proposed solution, telling that this technique can be effectively used in practical applications.

Kannan Karthik and Deepa Kundur, is described as Digital fingerprinting and video scrambling algorithms based on partial encryption. Necessary design tradeoffs for algorithm development are highlighted for multicast communication environments. We also propose a novel architecture for joint fingerprinting and decryption that holds promise for a better compromise between practicality and security for emerging digital rights management applications.

Wei Liu and Wenjun Zeng is described as Lossless compression of encrypted sources can be achieved through Slepian-Wolf coding. For encrypted real-world sources such as images, the key to develop the compression efficiency is how the source dependency is exploited. Approaches in the literature that make use of Markov properties in the Slepian-Wolf decoder do not work well for greyscale images. In this paper, we propose a resolution progressive compression scheme which compresses an encrypted image progressively in resolution, such that the decoder can observe a low-resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level. Excellent performance is observed both theoretically and experimentally.

Liang Zhou, Xinbing Wang,is describes as An important issue of supporting multi-user video streaming over wireless networks is how to optimize the systematic scheduling by intelligently utilizing the available network resources while, at the same time, to meet each video's Quality of Service (QoS) requirement. In this paper, first construct a general distortion model according to the network's transmission mechanism, as well as the rate distortion characteristics of the video. Then, we formulate the scheduling as a convex optimization problem, and propose a distributed solution by jointly considering channel assignment, rate allocation, and routing. Specifically, each stream strikes a balance between the selfish motivation of minimizing video distortion and the global performance of minimizing network congestions.

Jianwei Su and Xingming sun et al describes that wireless sensor networks are self-organized and data-centric, it have been applied in many practical areas. but data integrity protection strategy is based on the digital watermarking system, then one way hash function for collected data to create the water mark information then it associated with the data by embedding it into the redundant space of the binary byte. it is designed to extract the watermarking information, which is compared to recalculated watermarking information to verify the integrity of the data transmission. it does not increase excess data storage space and remain data accuracy. the result of extensive experiments, our algorithm can protect effectively in the integrity of the data in the more application values.

III. METHODOLOGY

TRIPLE DES ENCRYPTION STANDARD

Triple DES algorithm is a symmetric key block, the data encryption standard applies the cipher algorithm three times to each data block. It is three times slower than regular DES. But it is billion of time more secure when it used properly. Triple DES much wider use than DES because DES is so easily breaks today's technology. That any organizations with moderate resource can break through DES with les effort in these days. There is no same security expert would consider using DES to protect data. Triple DES was recently used for more secure than the DES. It is based on the DES algorithm; it is very easy to modify existing system software to use the triple DES.

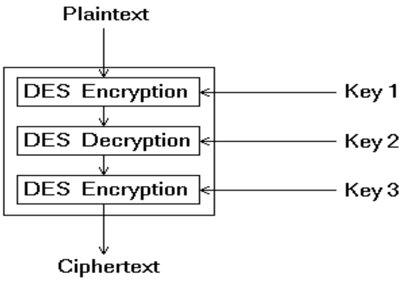


Fig no 1: Triple DES method diagram.

MULTI WATERMARKING OR DIGITAL WATERMARKING

A digital watermarking is embedded in a noise signal such as audio, video or images. It used to identity ownership of the signal. "Watermarking" is the process of hiding information of digital in a carrier signal; hidden file should not contain a relation to the carrier signal. Digital watermarking (or) multi watermarking used to verify the authenticity of the carrier signal to identify of its owner. Since a digital copy of data is same as the real or original, digital (or) multi watermarking is a passive tool of an protection. It does not control access the data.

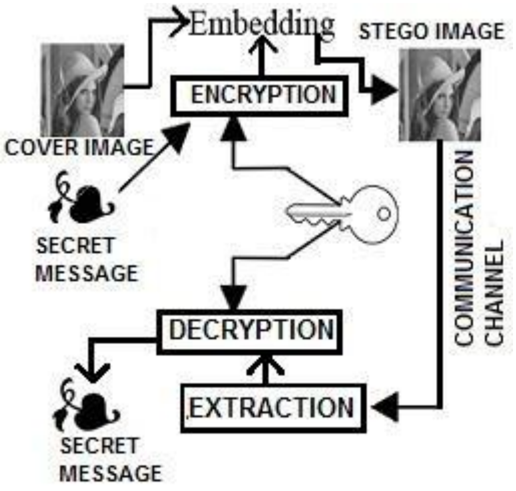


Fig no 2: Image Encryption and Decryption method diagram.

In this diagram, we explain about the process of embedding process of image in encryption and extraction process in the decryption into an image. Through this method we can send the important message to the other user.

IV. RESULT AND DISCUSSION

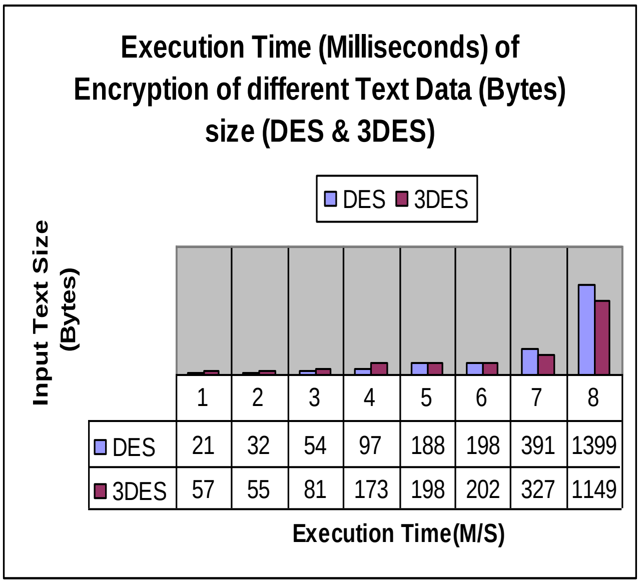
The following **Table 6.1** describes experimental result for proposed system algorithms. The table input text size for DES and 3DES algorithms for encryption execution time are shown.

Table no 1: Execution Time (Milliseconds) of Encryption of Different Text data size (DES & 3DES)

Input Text Size (Bytes)	DES	3DES
75	21	57
96	32	55
112	54	81
286	97	173
359	188	198
600	198	202
951	391	327
5345	1399	1149
Throughput (MB/sec)	**3.01**	**2.8**

It describes experimental result for proposed system algorithms. The table input text size for DES and 3DES algorithms for encryption execution time details

Fig no 3: Execution Time (Milliseconds) of Encryption of Different Text Data Size (DES and 3DES)



V. CONCLUSION

The objective of this paper is design of reversible watermarking technique for an relational data that ensure the recover the data without any compromising data quality. RRW detects that watermark were fully recover the original data. Data can recover in low key and high key extraction. Low key extract the low quality data or some data only. But the high key extracts the high quality data or over data. its mainly useful for the hospital management.

VI. REFERENCE

1. A. Cheddad et al.: “Digital image Steganography: Survey and analysis of current methods”, Signal Processing, Elsevier, 90(2010) 727-752.
2. B. Pfitzmann: “Information hiding terminology”, Information Hiding: First International Workshop, Cambridge, U.K., May 30 - June 1, 1996. Proceedings (Lecture Notes in Computer Science) , pp. 347-350, ISBN 3-340-61996-8.
3. T. Aura, “Invisible Communication”, EET 1995, technical report, Helsinki Uni. Of Technology, Finland.
4. W. Bender et al., “Techniques for Data Hiding”, IBM Systems, Vol.35, No.3 & 4, 1996, pp. 313-336.
5. Fabien A.P. Petitcolas et al., “Information Hiding – A survey”, Proceedings of IEEE, Special Issue on protection of multimedia content, 87(7):1062-1078, July 1999.
6. http://en.wikipedia.org/wiki/Covert_channel
7. M.H. Shirali-Shahrez, M. Shirali-Shahrez, “A New Synonym: Text Steganography”, Intl Conf. on Intl Info. Hiding and Multimedia Signal Processing, 978-0-3278-3/08, 2008 IEEE.
8. Kan Farhan Rafat et al: “Survey Report- State of the art in digital Steganography focussing ASCII text Documents”, IJCSIS, Vol.7, No.2, 2010.
9. Vidyasagar M. Potdar et al., “A Survey of Digital watermarking Techniques”, 3rd IEEE Intl Conf. on Industrial Information (INDIN), pp. 709- 716, 2005 IEEE.
10. M.D. Swanson et al., “Robust Data hiding for images”, 7th Digital Signal Processing Workshop (DSP 96), pp. 37-40, IEEE, Loen, Norway, Sep. 1996.
11. Minati Mishra et al., “IMAGE ENCRYPTION USING FIBONACCI-LUCAS TRANSFORMATION”, International Journal on Cryptography and Information Security (IJCIS), pp. 131-141, Vol.2, No.3, September 2012.
12. RC Gonzalez, RE Wood: Digital Image Processing, 2nd Ed, PHI, New Delhi, 2006.