ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 6, June 2013

Adaptive Video Watermarking With Multiple Cryptographic Salts

Krishan kant Lavania[1] , Chandresh Bakliwal [2], Megha Rathore[3] , Ashish Dadich[4]

Associate Professor, Arya Insitute Of Engineering and Technology, Kukas, Jaipur, India[1]

P.G.Student, Arya Insitute Of Engineering and Technology, Kukas, Jaipur, India[2]

P.G.Student, Jagannath Institute of Technology, Jaipur, India[3]

Associate Professor, Arya Insitute Of Engineering and Technology, Kukas, Jaipur, India[4]

Abstract: A new technique for transmitting the required secret information by embedding the information into the video after encryption through Salt Cryptography. A 512 bit key value is determined for encryption and positioning of secret information in the video. The encryption will be done depending upon a password. But along with the password some pseudorandom Salt sequences are also there. We will define salts which are random numbers needed to access the encrypted data, along with the password. If an attacker does not know the password, and is trying to guess it with a brute-force attack, then every password he tries has to be tried with each salt value. So, for a one-bit salt (0 or 1), this makes the encryption twice as hard to break in this way. A two bit salt makes it four times as hard, a three bit salt eight times as hard, etc. You can imagine how difficult it is to crack passwords with encryption that uses a 32-bit salt!. Salts are stored separately from passwords. That way, even if an attacker steals the password database, it is almost useless to him (if the salt has a lot of bits). The purpose of a salt is to add arbitrary random data to the string being hashed, such that you increase the length of input to hash.

Keywords: encryption, salt cryptography, 512 bit key, 32 bit salt, hash

I. INTRODUCTION

The digital watermarking is technique of embedding the hidden information into original data. There may be different way of embedding the watermark (hidden information) into host data such as embedding in spatial domain, transform domain and fractional domain[1][2]. The concept of digital watermarking consists of inserting information into the host signal under the situation that the modifications are not detectable. In addition, it is desirable to put maximum power into the watermark in order to reach high robustness. The signal energy must be maximized to decrease the error rate, this is a well known concept from communication theory. In mathematical formulation, the watermark embedding process can be considered as a constrained maximization problem i.e. to maximize the watermark energy under the visibility constraint. Although the problem is easy to formulate, it is tremendously difficult to implement because of the visibility constraint, which is generally based on a non-linear model of the human visual system. A perfect vision system is defined as one that has the capability to distinguish even the slightest changes in visual stimuli. For the human visual system this is, however, not the case. Digital watermarking is only achievable because our vision system is not ideal. The deficiencies in detecting certain stimuli or changes in stimuli have been extensively investigated in the past. Models to describe some of the visual effects, such as contrast sensitivity and masking, have been proposed, but for the moment no accurate mathematical description has been found that would allow simulating the full functional range of the human visual system.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 6, June 2013

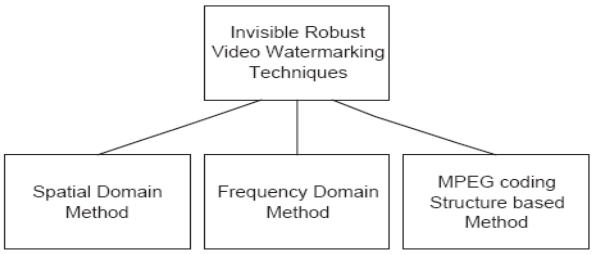


Figure 1: Classification diagram of existing digital video watermark techniques

Watermark embedding can be performed in a variety of ways as shown in figure 1. There are two main groups of watermark embedding technologies: coefficient-based and system-based. Coefficient-based approaches are the most obvious approaches since the embedding process is performed by a direct modification of pixel values or transform coefficient values[4-7]. Examples of this group are approaches based on pixel modifications in the spatial domain, such as least significant bit watermarking where the least significant bit of the pixel values are replaced by the binary watermark values. Extensions of this basic idea are based on spread spectrum communications and can be applied to a variety of domains a variety of domains, such as the frequency domain and wavelet domain. Recently, watermarking in the space/spatial-frequency domain has been defined[8-13].

In this paper we are proposing method that uses multilevel watermarks instead of a single organization watermark. These watermarks are independent of each other but individually identify the movie. Embedding algorithm has been developed as such all the three watermarks are not embedded together. The watermarks are embedded into different frames. The frame selection to embed a particular watermark is dependent on the other watermark. So we create some sort of dependence on each other for entirely independent watermarks.

This paper arranged as follows. In Section II, Frame video watermarking Technique and attacks are introduced, In Section III , Proposed algorithm for Primary, Secondary and Ternary Frames , Comparisons between different original frames and watermarked frames in Section IV. Finally In Section V, conclusions are drawn and future work is presented.

II. FRAME VIDEO WATERMARKING AND ATTACKS

The watermarks will be embedded into multiple frames for better security. Three frames will be selected on the basis of the watermark keys. Each of these frames will have specific information that will lead to identification of the pirated video at different levels.

A. Different Watermarks in different Frames

The watermarks namely the video and theatre IDs are stored in different frames in multiple copies. The frame selection we will discuss in next section. Once the frame indexes are known they are categorized as primary, secondary and tertiary level frames. This hierarchy is on the basis of information stored in them.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 6, June 2013

B. Watermark Dependent Frame Selection

The frame selection is done in a hierarchy. Three different classes in the hierarchy and the secret information contained in them are listed below:

- Primary Level Frames: These are the frames identified the movie ID. A modulo hash is performed on the movie ID using the number of frames in the entire video. This is selected from the first half of the video.
- Secondary Level Frames: The location of these frames is selected using modulo hashing has on the video ID. The hashing value gives the index of the secondary frame in the entire video sequence. This frame stores the theatre ID. So we are planning to store cross information pattern. Both the IDs are related to each other and we have used these related IDs as one to locate the other.
- Tertiary Level Frames: These frames will store the video ID and will be identified by modulo hashing of the theatre ID. Again cross information storage has been used. The frame selected by theatre ID and information inserted is video ID. This approach makes the security more robust.

Once the primary frame has been extracted it will tell about the other two keys and consequently the indexes of the secondary and tertiary frames.

C. Attacks on the Watermark Video

There are various attacks that can be applied on any cryptographic system especially when some data is hidden into the medium. Here we will discuss these attacks in context of secret data hiding in the video only[14-18]. Major attacks on video Stenganographic systems are listed below:

- **Frame Deletion Attack-** In frame deletion attack, the attacker deletes frame for the original message. The lost watermark can be recovered even after any number of frames gets deleted since the frames associated with watermark have been backed up properly. So a simple correlation can let us know which the frame the watermark was was embedded.

- **Forgery Attack**- In forgery attack the original watermark is captured by the eavesdropper which in turn transmits another message in place of the original one. This way the communication parties are not able to communicate properly. In our method some eaves dropper cannot forge the data since this will change the CRC of the video frames and ultimately CRC fail will occur leading to rejection of the video.

- **Eavesdropping**- An eavesdropper or adversary is a malicious entity whose goal is to prevent the communicating parties from achieving their objectives. An eavesdropper attempts to discover secret data between communicating parties, spoofing the identity of sender or receiver, distorting the transmitted data, sending malicious information in place of original messages. We prevent eavesdropping by simply the password authentication combined with the salt cryptography. The password alone is not capable of localizing the data in the video. It requires the salt to be combined with the password to get the exact location but this salt has been received from third party for registered users only. So the eavesdropper cannot know the exact locations of the message.

- **Brute Force attack**- In this attack the attacked tries for all possible permutations of the frame pixels to get the message, but we don't embed the actual message bits into the video file. We only embed the randomized mean values in the video which are in intensity domain like the other pixels. So mathematically it is impossible to predict the EDD values and to retrieve the message without knowing the exact embedding locations.

- **Malicious communicating parties**- If any of the communication parties are malicious then they can share the secret information. But in our proposed methodology all the information is not known to a single party. All the parties know only their domain of information. So even if they leak their part of information then the secret data is secured since the secret data from other parties also required for retrieval of the secret message from the video.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 6, June 2013

III. ALGORITHMS

The steps of the algorithm can be summarized in the following steps:

1. Authenticate the administrator
2. Input movie name and ID1=movie ID
   a. Convert movie ID into binary string
3. Load the original video
4. Gather parameters of the video
   a. Nframes=Number of frames in the video
   b. Height= Height of the video
   c. Width= Width of the video
5. Input ID2=video ID and ID3=theatre ID
   a. Convert the IDs into binary string
   b. Join the string

A. Primary Watermark Insertion

1. Prepare primary frame
   a. Primary frame will be located by the modulo of the movie ID by Nframes
   b. Modulo(ID1,Nframes)
   c. Backup original primary frame
2. Prepare primary watermark
   a. Join binary ID2 and ID3 = joint ID
3. Prepare salt to mix with ID1 to localize frame
   a. Third party interference to make the random salt corresponding to movie ID
   b. Length of salt = Bit length of the joint ID
   c. Width of salt = *log(Height* Width) – 1*
4. Watermark Insertion indexes localization in a Primary frame
   a. Salt is mixed with the movie ID.
   b. Decimal value of the salt gives the location in the primary frame to embed the watermark.
5. Watermark Insertion
   a. Embedding positions are localized by the final combined salt
   b. Watermark embedding method explained in previous section is used for watermarking
   c. The primary frame in the video is replaced with this watermarked video frame
   d. Back up of the primary watermarked video frame

B. Secondary Watermark Insertion

1. Prepare secondary frame
   a. Secondary frame will be located by the modulo of the video ID by Nframes
   b. Modulo(ID2,Nframes)
2. Prepare secondary watermark
   a. binary ID3 = theatre ID
3. Same salt will be used
4. Watermark Insertion indexes localization in a secondary frame
   a. Salt is mixed with the video ID.
   b. Decimal value of the salt gives the location in the secondary frame to embed the watermark.
5. Watermark Insertion
   a. Embedding positions are localized by the final combined salt
   b. Watermark embedding method explained in previous section is used for watermarking
   c. The secondary frame in the video is replaced with this watermarked video frame
   d. Back up of the secondary watermarked video frame

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 6, June 2013

C. Tertiary Watermark Insertion

1. Prepare tertiary frame
   a. Tertiary frame will be located by the modulo of the theatre ID by Nframes
   b. Modulo(ID3,Nframes)
2. Prepare tertiary watermark
   a. binary ID2 = video ID
3. Same salt will be used
4. Watermark Insertion indexes localization in a tertiary frame
   a. Salt is mixed with the theatre ID.
   b. Decimal value of the salt gives the location in the tertiary frame to embed the watermark.
5. Watermark Insertion
   a. Embedding positions are localized by the final combined salt
   b. Watermark embedding method explained in previous section is used for watermarking
   c. The tertiary frame in the video is replaced with this watermarked video frame
   d. Back up of the tertiary watermarked video frame

Multiple iterations of the primary secondary and tertiary watermarking can be done with different selection of frames to increase the security but this may increase some noise in the original video after certain limit

D. Watermark Extraction

The process given in the watermark embedding section is completely reversed to dig out the watermark from the video frames. The major steps involved are:

1. Input the watermarked video
2. Input movie ID
3. Generate primary frame index
4. Generate salt corresponding to movie ID
5. Mix salt and movie ID to get watermarked pixel indexes in the primary, secondary and tertiary frames
6. In primary frame search for hidden info
7. This info is joint ID composed of the video ID and theatre ID
8. Both the IDs are extracted from the joint ID
9. Secondary and tertiary frames' indexes are calculated
10. Hidden information in these frames is matched with the video and theatre IDs.
11. If matched then claim can be done.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 6, June 2013

IV. COMPARISONS BETWEEN DIFFERENT ORIGINAL FRAMES AND WATERMARKED FRAMES

Histogram Comparison of the Frames

A. Primary

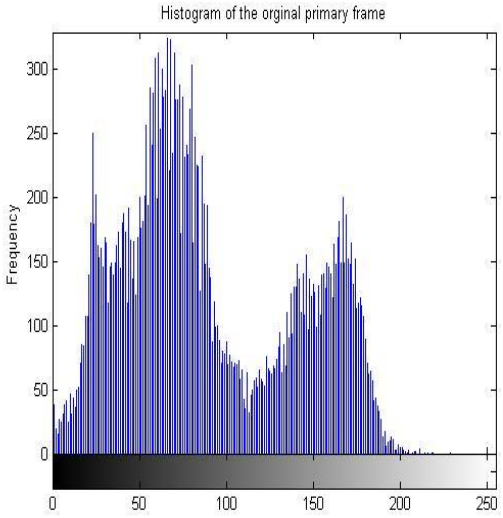


Figure 2: Histogram of the original primary frame

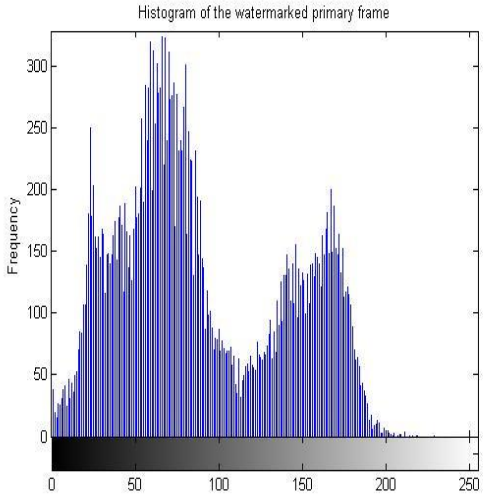


Figure 3: Histogram of the watermarked primary frame.

B. Secondary

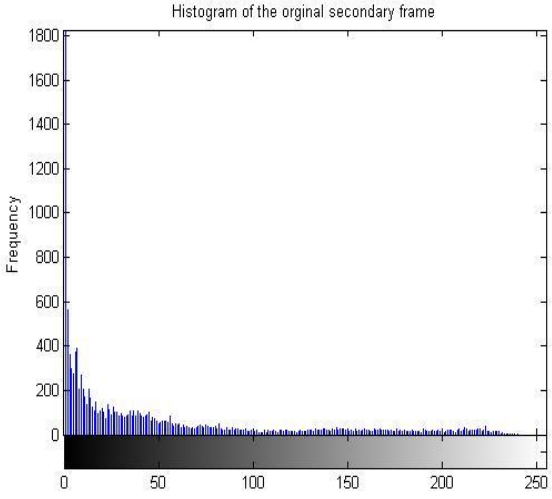


Figure 4: Histogram of the original secondary frame.

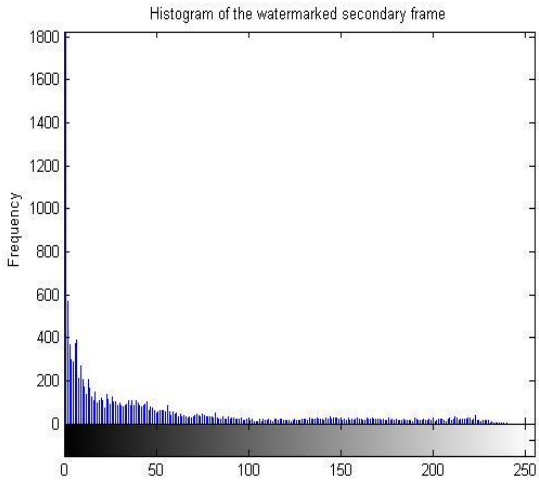
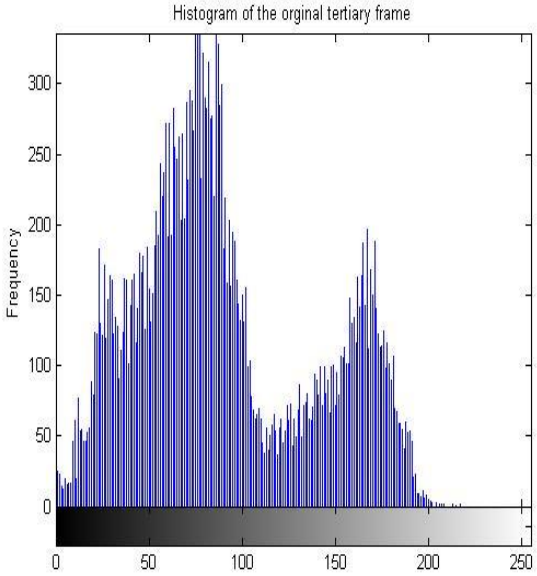


Figure 5 : Histogram of the watermarked secondary frame.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 6, June 2013

C. Tertiary



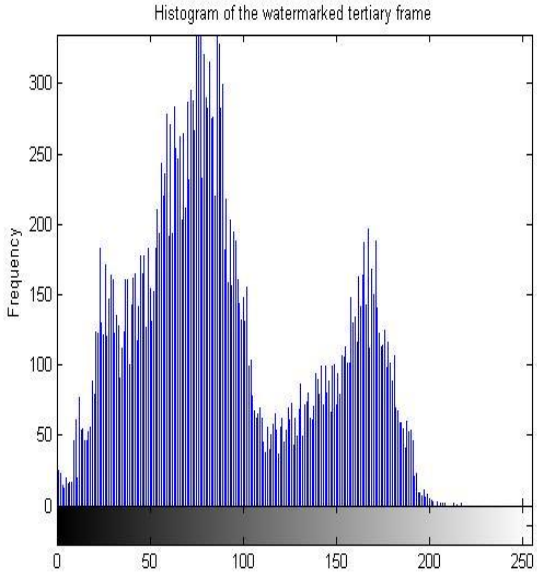


Figure 6 : Histogram of the original tertiary frame.

Figure 7: Histogram of the watermarked tertiary frame.

V. CONCLUSION AND FUTURE WORK

It is clearly visible from the histogram comparison of the original and watermarked frames that there is no noticeable difference in the peaks of the histogram. This is because of the use of the mean of the neighborhood watermark. This mean shows no visible effect on the images. This scheme is novel in this area and has no algorithmic comparisons. The concept of salt cryptography for video watermarking is totally novel. The watermarking information is stored in the frames. Multiple levels of information have been used as watermarks. Different levels of information have been embedded in different frames. The frame number to embed the watermark is calculated from the video, movie and theatre ids. The original frames and the watermarked frames are also stored by the verification authority. The proposed algorithm is robust against frame deletion attack. Even large number of frames are deleted the watermark can be detected by simple correlation with the video frames. The results are very good as there is no visual change in the Stego video . The main idea to check the hidden data i.e. histogram checking is also not able to detect the presence of the data. So overall this approach is successful landmark for data hiding in the videos. We are planning in future to include some frequency domain transforms to make it comparable with other techniques in the frequency domain.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 6, June 2013

REFRENCES

[1] A. J. Menezes, P. C. Van Oorschot, and S. A.Vanstone, Handbook of Applied Cryptography,Boca Raton, CRC Press, 1996.

[2] D. Kahn, The Code breakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet, 2nd ed.,New York: Scribner, 1996.

[3] A. Kerkhoffs, "La Cryptographie Militaire," Journal des Sciences Militaires, 9th series, pp. 5–38, 161–191 January/February 1883.

[4] C. E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, Vol. 28, No. 4, pp. 656–715 October 1949.

[5] C. A. Devours, Selections from Cryptologia: History, People, and Technology, Norwood, MA: Artech House, 1998.

[6] I. J. Cox, Secure Spread Spectrum Watermarking for Multimedia, NEC Research Institute, Tech.Rep.95-10, 1995.

[7] W. Bender, "Techniques for Data Hiding," IBM Systems Journal, Vol. 35, Nos. 3 4, pp. 313–336, 1996.

[8] I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking, The Morgan Kaufmann Series in Multimedia Information and Systems, San Francisco:Morgan Kaufmann Publishers, 2002.

[9] M. Kutter, F. Hartung, S.C. Katzenbeisser, "Introduction to Watermarking Techniques", Information Techniques for Steganography and Digital Watermarking, Eds. Northwood, MA: Artec House, Dec. 1999.

[10] Inoue H., Miyazak A.,Katsura T.,"An Image Watermarking Method Based on the Wavelet Transform," Kyushu Multimedia System Research Laboratory.

[11] I. J. Cox, M.L. Miller, J.M.G. Linnartz, T. Kalker, "A Review of Watermarking Principles and Practices" Proceedings of SPIE, Human Vision & Electronic Imaging II, vol. 3016, pp. 92-99, February1997.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 6, June 2013

[12] F. A. P. Petitcolas ,"Watermarking Schemes Evaluation", IEEE Signal Processing Magazine, Vol 17, pp 58-64, September 2000.

[13] E. Koch, J. Zhao, I. Pitas, "Towards Robust and Hidden Image Copyright Labelling," Proceedings of 1995 IEEE Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, Greece, pp. 452–455, June 1995,.

[14] G. Langelaar, I. Setyawan, R. Lagendijk, "Watermarking Digital Image and Video Data ",in IEEE Signal Processing Magazine, Vol. 17, pp. 20-43, Sept. 2000.

[15] Jiwu Huang,Yun Q.Shi," Embedding strategy for image watermarking in DCT do-main" in Asia-Pacific Conference on Communications , Vol.2 , , China, pp.981-984,Oct. 1999

[16] Ying Li, Xinbo Gao, Hongbing Ji," A 3D wavelet based spatial-temporal approach for video watermarking "in Proc. IEEE Int. Conf. on Computational Intelligence and Multimedia Application, pp.260- 265,27-30 Sept. 2003

[17] F. Hartung and B. Girod, "Digital Watermarking of MPEG-2 Coded Video in the Bit stream Domain", in Proc. IEEE ICASSP, pp. 2621-2624, April. 1997.

[18] K. V. Arya, Lovelesh Saxena, Anuj Tewari "A Novel Technique for Secure Information Transmission Using Framed Video Watermarking" In Springer image Processing and Communications Challenges 3 Advances in Intelligent and Soft Computing Volume 102, 2011, pp 245-256