International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Robust Sterilization Resistant Video Authentication using Pixel Randomization and Modified Lsb Steganography

Jayati Bhadra, M. Vinayaka Murthy, M.K. Banga

Abstract*: *An authentication method which uses randomization of the pixel selection and keyless modified Least significant bit steganography of a video is proposed. Randomization of pixel selection for hiding authentication information is based on probability percentage of the red color intensity values of each pixel of image frame, is not considered in any of the existing methods. The proposed method also uses modified LSB steganography which reduces the cost due to its simplicity. This method ensures minimum alterations of the resultant image. Keyless invisible embedding process increases the security. Experiments using histogram, surface plot proved that it can withstand visual attack. Euclidean distance, Chi-square, Correlation, Intersection values proved that it can withstand statistical attacks. StirMark benchmark test for robustness is used to prove that the proposed system is highly robust. This proposed method of video authentication gives cost effective solution which is better than the existing methods.

Keywords* : *modified LSB, video steganography, probability percentage, randomization

I. INTRODUCTION

Nowadays a large number of images/videos are being transmitted over internet which is not secured[13]. So, the copyright protection is the most important aspect. This can be done by various forms using different mechanisms. To maintain transmitted data to be extremely secured, it is required to develop a system more robust and imperceptible. In the field of data security, data hiding plays a very significant role. A color video is a collection of a set of still color image frames and audios. Each frame contains pixels.

Manuscript published on 30 September 2019
* Correspondence Author
Ms. Jayati Bhadra*, Assistance Professor, Computer Science,
Dr M Vinayaka Murthy, Professor, Department of Mathematics, REVA University.
Dr. M.K Banga, Professor, Department of Computer Science and Engineering at J N National College of Engineering, Shimoga

Each pixel is having set of RGB color intensity information bits[14]. LSB steganography is the most common, simple but effective method in Spatial Domain steganography. Though it has low computational complexity, it gives low security. To increase the level of security, randomization of pixel selection to embed the data and modified LSB is introduced in this paper.

Also the pixel values of Red color channel of the frames are used for data hiding and Probability Percentage of the Red color pixel values are used for the selection of randomized pixels. Thus the proposed method increases the security of the hidden copyright information. This imposes low distortions and high opposition to the removal of copyright information. In this paper, section II explains literatures reviewed, section III gives a clear idea about the proposed method, section IV documents the experimental results, section V concludes the paper.

II. REVIEW OF LITERATURE

Steganography is a process of inserting sensitive data inside a media. Though it is simple, it helps implementing security with robustness and better recovery of secret data. Yunxia et al [3] reviewed different video steganography method and concludes that based on pixel selection, there are intra, pre and post embedding methods. They also pointed out the challenges of these methods with respect to security and robustness. Moon et al [4] proposed a process which conceals the image-frames and audio-data as secret data inside the arbitrarily selected video-frames using "Multi Frame Exploiting Modification Direction (MFEMD)" Algorithm. Though it is really challenging to extract hidden data, forensic tool is used to decode the information. This increases the time-complexity of the system. Manisha et al[2] proposed a novel technique to hide secret information in an video. Here an image-frame is used as cover before hiding inside the video image frame. The secret information will be encrypted in two levels and then will be hidden in Bitmap image. So the process of hiding information will be time consuming and in turn, increases the cost. Biswas et al[1] proposed, a hybrid cryptography using AES and RSA. Encrypted symmetric key, encrypted secret message and digital signature based on secret message together will be sent to the receiver after hiding it into the cover media using LSB steganography.

Both AES and RSA need multiple rounds processing which is computational time heavy method. Also the symmetric key is vulnerable to eavesdropping.

III. PROPOSED METHODOLOGY

Any video is composed of audio and image frames. A short text message as an authentication information of the video can be hidden inside the image frame to protect from piracy in spatial domain. In this proposed method, each image frame will be the cover media and actual image content is used to find the probability percentage of the red color intensity of the pixel for each row. After finding the highest and lowest probability percentage, mean of these two values will give the intensity of the red color channel of the pixel to hide the bits of the text message. So, each video consists of $\{I_i, i=1,2,\ldots.k\}$ image frames where k is the overall image frames in the selected video.

Therefore,

$$Video = \sum_{i=1}^{k}(image\ frame)_i + audio\ track \quad (1)$$

Each image frame has r rows and c columns. Therefore,

$$image\ frame\ (I) = r \times c \quad (2)$$

Each image frame consists of pixels with pixel values $X_{i,j}$ *where* $i=0,1,\ldots\ldots,r$ *and* $j=0,1,\ldots\ldots,c$, *i.e.,*

$$image\ frame\ I = \sum_{i=0}^{r}\sum_{j=0}^{c}X_{i,j} \quad (3)$$

Each image frame (I) has three channels of color intensities Red(I_r), Green(I_g) and Blue(I_b). Here, actual image content is used to find the probability percentage(PP) of the red color intensity of the pixel for each row.

The *Probability Percentage*(PP) of pixel intensity is defined as follows

***Definition* :** The probability of the red color intensity of the pixel is the ratio between red color intensity (I_r) and the maximum value of the red color intensity (255). Then the *Probability Percentage*(PP) is 100 times the probability.

Let red color intensity be I_r , then Probability of red color intensity =(I_r / 255)

So, the *Probability Percentage*(PP) = 100 x (I_r / 255) (4)

In this proposed method, mean of highest and lowest PP will be calculated for each row and the pixel position whose red color intensity value is same will be selected to hide data. If PP_i is the *Probability Percentage* of the red color intensity of a pixel in i^{th} row,

Then, Mean of PP_i = (highest(PP_i) + lowest(PP_i))/2 (5)

If the mean value is not exactly same, the closest value will be considered for pixel selection.

The proposed algorithm — modified LSB steganography with Randomized pixel selection is as follows:

Step 1 - AVI video can be selected as cover media. Short text message as authentication information will be selected and will be converted into binary form.

Step 2 - The selected video will be segregated into a sequence of bitmap image frames and audio. Each frame consists of three channels of Red, Green, Blue [5].

Step 3 - The Red color intensity value of pixels of each frame will be copied in an array(list is used in case of Python implementation).

Step 4 - Using Eq. (5), value of mean will be calculated for each row. The location vectors will be selected based on mean value(or close to mean value).

Step 5 - The last but one ie, 7^{th} bit of the red channel pixel intensity value of selected location vectors will be replaced by the bits of text message.

Step 6 - After hiding the text message in all the frames, rejoin the image frames and the audio to get the stego video, which is authenticated.

Step 7 - At the receiver's end, the same algorithm is used to locate the pixel. After locating the pixels the hidden text bits can be extracted using modified LSB steganography method.

IV. RESULTS

50 different AVI videos from Archive.com as cover media, are used for the testing of the algorithm. From the results, it is clear that the proposed video authentication process is resistant to visual and statistical attacks. In particular, image part of the video is used to hide information. Image frames will be in BPM format.

The main reasons for choosing the video format as AVI

1. Players and devices can support
2. Image frames are of high resolution

The main reasons for selecting the image format as BMP are :

1. Quality of the image is very good
2. Modification and edition can be done easily
3. Lossless process. Colour image frames are used for randomization of the pixel in place of gray scale frames. Probability percentage concept is used for randomization which is unique. Time complexity for randomizing the pixel positions is O(nlogn) and hiding the bits using modified LSB is O(n). So time complexity of this proposed method is

$$O(nlogn) + O(n) = O(nlogn) \quad (6)$$

Eq. (6) proves that the time complexity is increased compared to the time complexity of the modified LSB. In turn, security of the system also increased. Moreover, the time complexity of DCT and DFT in transform domain is $O(n^2)$ which is higher than our proposed algorithm. As the proposed method is keyless, data security is enhanced. Due to the simplicity of modified LSB method, computational time is also less. So the method is cost effective.

A. Robustness

Table 1. StirMark result for robustness

Name of the test	Value of Distortion	PSNR	Resultant Noise(dB)
Test_MedianCut	3	173.46	40.1901
Test_SelfSimilarities	1	172.57	41.0251
Test_RemoveLines	10	172.822	NA
Test_RemoveLines	50	172.722	NA
Test_Cropping	20	197.739	NA
Test_Rescale	50	172.875	NA
Test_Rotation	-2	159.874	NA
Test_Rotation	5	143.98	NA
Test_RotationCrop	-.5	173.18	NA
Test_RotationScale	.75	173.467	23.002
Test_Affine	8	169.22	NA
Test_LatestSmall Random Distortions	1.1	167.53	19.61
Number of tests which failed	NILL		

Robustness refers to maximum data amount that may be hidden into the host video without fidelity losing. Using our proposed method, we will be storing the authentication information in every frame. We have used StirMark [6-8], which is a standard benchmark tool for checking whether the steganographic and watermarking algorithms used on the image is robust or not. When an image is photocopied, printed or rescanned, there will be some distortions after photocopy/reprint/rescan in the resultant image. Same way, the attack simulates image distortions. that generally take place when an image is photocopied, printed or rescanned there will be some distortions after photocopy/reprint/rescan in the resultant image. StirMark simulates image distortions of that type and checks whether the distorted image is robust or not. We executed StirMark 4.0 on the image frame and the result that shows none of the test are failed. So the proposed embedding process is robust.

B. Resistance to Statistical Attack

By implementing Westfeld and Pfitzmann's test [9] we can prove that the proposed algorithm is resistant to first order statistical *attacks*. Also Provos et al. [11] proved that the color frequency test is not effective if the information is hidden in randomly selected pixels though it will work well if the information is hidden sequentially. We are not starting the hiding process from the beginning of the image frame and the proposed process of hiding is not chronological based on pixel positions, it can withstand this test. Proposed algorithm can withstand *duel statistics test* as flipping of LSB in this test will not be effective. In our proposed method, we are using the last but one-th bit ie, 7^{th} bit position to hide the message bit in pixels at random positions in the image.

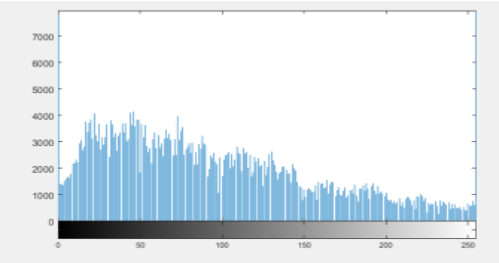

Fig. 1.Histogram of Frame5 of out.avi

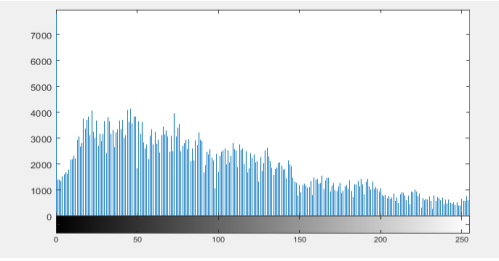

Fig. 2. Histogram of Frame5 of out.avi with authentication information

Table 2. Comparison of two histograms of original and with authentication information

Euclidean Distance	Correlation	Chi-square	Intersection
$2.5804e^{-10}$	0.302	3.523	0.403

From Table 2, it is clear that the cover and stego frames are very similar as Euclidean distance between the histograms is very small, correlation is less than one, chi-square test shows strong similarity, the intersection of two histograms is small, which established that the proposed method is visual attack resistant.

The difference between means of cover frame and the frame with authentication varies from .0001 to .0010, which is very small. Similarly the standard deviation of cover frame and the frame with authentication varies from 0001 to .0006, which is again very small. Both these difference value ranges tell us that the original frame and the frame with hidden authentication message very similar to each other. So from Fig. 1, Fig. 2 and Table 2, the comparative values prove that the two frames are very close to similarity.

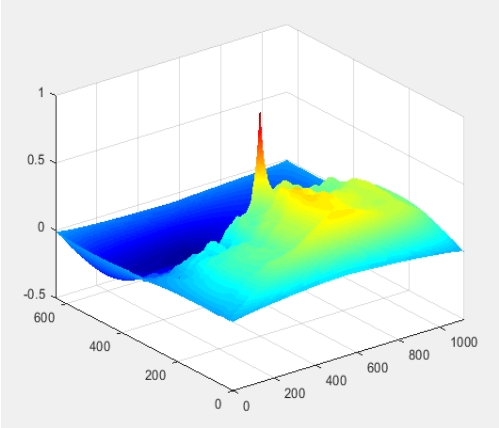

Fig. 3. NCC of original Frame 5

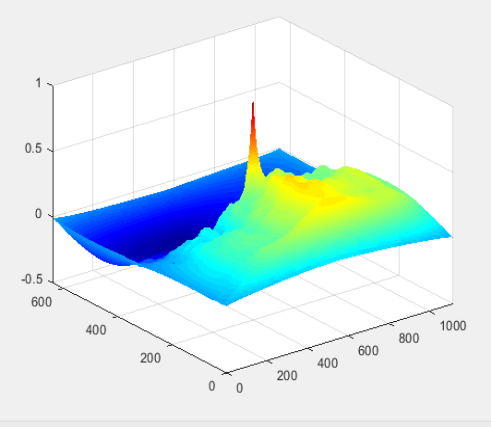

Fig. 4. NCC of stego Frame 5 of out.avi with authentication information

In Fig. 3 and Fig. 4, the Normalized 2-D cross correlation(NCC) of the image frame5 before and after the authentication information is embedded, we find no visual difference which proves the resistance to the visual attack. The hidden data is very difficult to extract without knowing the randomization logic which helps rise to the security of the proposed algorithm. Also it is difficult to detect using HVS as the quality of the stego image is very high. So we can say that the proposed method can withstand visual attacks.

C. Resistant to sterilization

It is difficult to detect the hidden data without having any prior knowledge of the embedding algorithm or the knowledge of the key used. The concept of image sterilization can be used to remove the hidden data from suspected image. To do so, we change the LSB from 0 to 1 and 1 to 0 for all the pixel values of the image frame. Here, we are storing the authentication information using modified LSB method where we are not storing the bits in LSB. So sterilization process will not be effective for our proposed method.

D. Analysis Through Quality Metrics

Image quality measurement – MSE, PSNR, SSIM

Mean Square Error(MSE)

MSE= $\frac{1}{M*N}\sum_{m=1}^{M}\sum_{n=1}^{N}[x(m,n)-y(m,n)]^2$, where M, N are rows and columns of image matrix, $x(m,n)$ is the original image, $y(m,n)$ is stego image.

If the value of MSE is greater than 0, then the stego image will be of poor quality.

Peak Signal to Noise Ratio(PSNR)

PSNR = 20. $\log_{10}$ [MAXPIX/RMSE] where

RMSE = $\sqrt{MSE}$ is the root mean square error, MAXPIX is the Maximum Possible pixel value of the image. If the PSNR has large value then the stego image is of good quality.

Structural Similarity Index Metric (SSIM)

SSIM = $((2a_xa_y + c_1)(2b_{xy} + c_2)/(a_x^2 + a_y^2 + c_1)(b_x^2+ b_y^2+ c_2))$

Where "a", "b", & "b_{xy}" are mean, variance, and covariance of the images, and "c_1, c_2" are the stabilizing constants. The value of SSIM will vary between 0 and 1. The value of SSIM for similar images will be near or equal to 1.

Table 3. Quality metrics of test videos

Video name	Resolution	Frames / sec	No. of Frames	AverageMSE	Average PSNR	Average SSIM
Out.avi	720X1280X3	25	125	.0020	77.5	1.0
Test_1.avi	320X870X3	20	120	.0034	78.3	1.0

In Table 3, we see that the average MSE value is less than 0, average PSNR value is more than 1 and average SSIM is less than equal to 1 which implies that the frames with authentication information is of good quality.

Table 4. Comparative study using same image

Paper detail	Concept used	PSNR value
Paul et al. [12]	Energy pixel	38.62
Proposed method	Probability percentage	78.73

In Table 4, we have seen in LSB implementation using similar type of concept called energy pixel by Paul et al. [12], PSNR value is 38.62 which less than our average PNSR value 78.73 on the same image. This shows that the proposed randomized pixel based watermark is better than the energetic pixel based watermark.

V. CONCLUSION

Here the time complexity of the algorithm is O(*n log n*) which shows that the complexity of the process is better than the Modified LSB which is O(n). So, it will give better security. The stego image quality is very similar to cover image as the *PSNR* value is high ,the MSE is very low, SSIM value is 1.0 . The difference between a cover and Stego image frame can be expressed using **h**istograms. But in this case, it is difficult for the human eye to recognize any difference. It is proved that the proposed system is robust using stirmark software. The proposed system is cost effective also, as the steganographic method used is simple compared to transform domain. Though, we can explore the same algorithm on transform domain also. Instead of uncompressed domain, compressed domain can also be explored. For faster processing, GPUs can be used.

REFERENCES

1. Chitra Biswas , Udayan Das Gupta, Md. Mokammel Haque : "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography", International Conference on Electrical, Computer and Communication Engineering (ECCE), 2019, DOI:10.1109/ECACE.2019.8679136
2. S. Manisha, T. Sree Sharmila : "A two-level secure data hiding algorithm for video steganography, Multidimensional Systems and Signal Processing", April 2018, Volume 30, Issue 2, pp 529–542
3. LiuYunxia, LiuShuyang, WangYonghao, ZhaoHongguo, LiuSi : "Video steganography: A review", 2018, https://doi.org/10.1016/j.neucom.2018.09.091
4. Sunil K. Moon, Rajeshree D. Raut : "Information security model using data embedding technique for enhancing perceptibility and robustness", 2019, https://doi.org/10.1504/IJESDF.2019.096528
5. Ozcan, C., Kemal, T. : "Comparison of LSB image steganography technique in different color spaces", In 2017 international artificial intelligence and data processing symposium (IDAP), 2017, (pp. 1–6). IEEE.
6. Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn: "Attacks on copyright marking systems", in David Aucsmith (Ed), Information Hiding, Second International Workshop, IH'98, Portland, Oregon, U.S.A., Proceedings, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, 1998, pp. 219-239
7. Fabien A. P. Petitcolas: "Watermarking schemes evaluation", *I.E.E.E. Signal Processing*, 2000, vol. 17, no. 5, pp. 58–64
8. http://www.petitcolas.net/fabien/watermarking/stirmark
9. Westfeld A, Pfitzmann A : "Attacks on steganographic systems", In: Proceedings the 3rd international workshop on information hiding, LNCS 1768. Springer-Verlag, 1999, pp 61–76
10. Fridrich J, Goljan M, Dui R : "Reliable detection of LSB steganography in color and grayscale images". In: Proceedings of the ACM workshop on multimedia and security, Ottawa, 2001, pp 27–30
11. Provos N : "Defending against statistical steganalysis". In: 10th USENIX security symposium, 2001, pp 325–335
12. Goutam Paul, Ian Davidson, Imon Mukherjee, S. S. Ravi, : "Keyless dynamic optimal multi-bit image steganography using energetic pixels", Multimed Tools Appl, 2016, DOI 10.1007/s11042-016-3319-09
13. A. StephenDass,J. Prabhu: "Comparative Analysis of a Systematic Coherent Encryption Scheme for Large-Scale Data Management Using Cryptographic Encryption Technique", Smart Intelligent Computing and Applications, ISBN 978-981-13-1927-3, 2018, pp 427-437
14. Arshiya Sajid Ansari, Mohammad Sajid Mohammadi, Mohammad Tanvir Parvez : "A Comparative Study of Recent Steganography Techniques for Multiple Image Formats", I. J. Computer Network and Information Security, 2019, 1, 11-25

AUTHORS PROFILE

MS. JAYATI BHADRA , Research Scholar, Assistance Professor and Coordinator
Ms. Jayati Bhadra earned her M.Phil from Madurai Kamaraj University, MCA from IGNOU, M.Sc. in Applied Mathematics from Jadavpur University, Kolkata. She has nearly 16 years of teaching experience in colleges/university. She served as Coordinator of M.Sc. in computer Science and M.Sc. in Big Data Analytics, St.Joseph's College(Autonomous) Bangalore. Her areas of research interest are Data security, Computer networks, Machine Learning and Data Analytics.

Dr M Vinayaka Murthy, Professor Having secured Ph. D. in "Computational Fluid Dynamics - Mathematics" from Bangalore University, M.Sc. in Mathematics, B.Sc. in Mathematics from Bharathidasan University and B. Ed. degree in Mathematics from Annamalai University, he has 27 years of teaching experience in UG, PG and PhD, teaching various subjects like Discrete Mathematics, Probability and Statistics, Operations Research, System Simulation and Modelling, Finite Automata Theory, Analysis and Design of Algorithms, Computer Graphics, Data Mining & Data Warehousing, Numerical Methods, Mathematics, Basic Mathematics and Research Methodology. He is recognized by as a Research guide in computer Science of University of Mysore, VelTech University and REVA University. He has published 50 and more research papers in reputed journals and conferences. He is interested in guiding research in Data Mining and image processing. He is guiding 8 PhD Scholars. Already 2 scholars are awarded PhD in Computer Science under his guidance in REVA University;

Dr. M.K BANGA Professor and Chairman Dr. M.K.Banga earned his Ph. D. in Computer Science from Indian Institute of Technology, Kharagpur, for his thesis on Parallel Processor Architectures. He has nearly 16 years of teaching experience in engineering colleges/university. He served as Professor of Computer Science and Systems Manager, at Bapuji Institute of Engineering and Technology, Davangere and later as Prof. and Head of the Department of Computer Science and Engineering at J N National College of Engineering, Shimoga, before joining Wipro Technologies, Bangalore. Prof. Banga served at Wipro Technologies for 14.5 years in various capacities including General Manager & Head of the Architect Academy for 2 years. He was Prof. & Head of the School of Computer Science & Information Technology for one year before joining Dayanand Sagar University. He has guided more than 15 M.Tech. Students for their project work and is currently supervising 6 research scholars for their Ph.D. degree. His areas of research interest are Data Networks, Wireless Ad-hoc Networks, Machine Learning and Analytics