IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.6, Special Issue.11, Dec 2018 E-ISSN: 2347-2693

Secure Data Hiding in Encrypted Video Using SVD

P.S.S. Akilashri[1*], M.Kannan[2]

[1]Dept. of Computer Science, National College, Tiruchirappalli, India
[2]RKV Matric Hr Sec School, Jedarpalayam, India

Available online at: www.ijcseonline.org

Abstract— Video data hiding is a very Abstract – Video data hiding is very important research topic. Security of information is major concern of information technology and communication. This paper introduces svd and Least Significant bit substitution technique for hiding data in video file. In this paper data hiding a form of cryptography embeds data into digital media for the purpose of identification, annotation. These algorithms are a basic algorithm of encryption and decryption for data hiding. The framework is tested by all kind of videos such as .mp4, .3gp, .avi etc., and gets successful output for all video data hiding process. The three components Red, Green, Blue of (RGB) space are utilized by this scheme to embed watermark into the cover image. Specifically the combinations of Singular Value Decomposition (SVD) of Blue channel are used to embed the data hiding. The singular values of wavelet subband coefficients of Blue channel are use in different scaling factors to embed the singular values of the data. The SVD increases the security, robustness and imperceptibility of the scheme. The proposed scheme used by security, while hiding the video to provide security for encrypts and decrypt process. The simulation results show that the process of hiding the video by security.

Keywords— Video Data hiding, Encryption, Decryption, Security Data, SVD.

I. INTRODUCTION

Data hiding involves embedding significant information into a variety of forms of digital media such as text, audio, image and video secretly. Applications of data hiding are copyright protection, fingerprinting and secret communication. The purpose of data hiding techniques is different from that of traditional cryptography or watermarking techniques. Traditional Cryptography encrypts messages into meaningless data while watermarking is utilized to protect the copyright. Data hiding technique covers the secret information with the host media as camouflage and is considered as an extension of traditional cryptography. The development of Internet technology that in development, people can transmit the data and share digital (images, video) content with each other conveniently and it is rapidly used. In order to guarantee communication (that is internet) efficiency and save the network bandwidth, efficiency, compression techniques can be implemented in digital components to reduce redundancy, noise and the quality of the decompressed should also be preserved. Most digital content, digital images and videos, are converted into the compressed form of transmission. To solve this problem in steganography technique is developed in both academia, industry and more. The goal of cryptography is to make text/information unreadable by a third party or attacker, whereas the goal of steganography is to hide the data from a third party or attacker.

Due to the speedy make use of of digital images on the Internet, how to reduce the images and hide the secret information into the compacted form of images efficiently deserves in depth study. There many data hiding schemes for compressed codes that it is applied to hide the data ,i.e stenography etc. which apply to various different compression techniques of images, that may be JPEG200, JPEG, Singular Value Decomposition(SVD). But digital images are most popular because of their usage on the internet. Different application uses different Steganography techniques on their requirements Lossy data compression techniques that create smaller image by discarding excess image pixel from the original image. SVD is used due to its simplicity and cost effectiveness for digital image compression. The Euclidean distance is taken to evaluate the similarity between the codewords in the codebook and image block for the SVD compression process. The block is represented, that is recorded which is having the index of the codeword with smallest distance. The index values containing in the table for all blocks are generated as code of SVD compression. And only index values are stored instead of pixel values. And through lookup table for each received index, that is a SVD decompression process

II. LITERATURE SURVEY

In this paper [1] sound is there in digital image throughout image acquirement, code, transmission, and processing ladder Noise is very complicated to take out it from the digital images without the prior facts of noise model. The advantage of this paper is a complete and quantitative

analysis of noise models available in digital image. Disadvantage of this paper is cannot be compressed. In this paper [2] this paper concentrates on the aspects and approaches of image hiding techniques and cryptosystem for digital images. Data hiding can be divided into two categories such as digital watermarking and steganography. The advantage is we can hide the data in image. Disadvantage is it is not perfect image.

In this paper [3] recently, different techniques are available for data hiding. When to send some confidential data over insecure channel it is mandatory to embed data in some host or cover media. The advantage of this paper is the data hider compress the image to create sparse space to accommodate some additional data. Disadvantage is it is difficult to handle. In this paper [4] this work proposes a novel Reversible Image Data Hiding (RIDH) scheme over encrypted domain. The information embed is achieve from side to side a public key modulation mechanism, in which access to the secret encryption key is not needed. Is able to perfectly reconstruct the original image as well as the embedded message. Need to, contain a relation to the carrier signal.In this paper [5] the transmission of confidential data over the network requires more security. So, for improving security in data transmission, we can hide the data inside an encrypted image. Reversible Data Hiding. The original image can be recovered lossless.

III. METHODOLOGY

ALGORITHM SVD:

The **singular value decomposition** is a factorization of a real or complex matrix. It is the generalization of the eigen decomposition of a positive semi definite normal matrix (for example, a symmetric matrix with positive eigenvalues) to any m X n matrix via an extension of the polar decomposition.

It has many useful applications in signal processing and statistics.

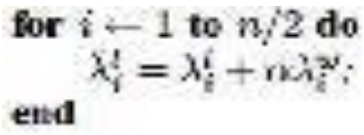
- The left-singular vectors of **M** are a set of orthonormal eigenvectors of **MM∗.**
- The right-singular vectors of **M** are a set of orthonormal eigenvectors of **M∗M**.
- The non-zero singular values of **M** (found on the diagonal entries of Σ) are the square roots of the non-zero eigen values of both **M∗M and MM∗**

Vide Data Hiding Encode

Input: The colour image I of size m x n and the monochrome video W of size m/2 x n/2

Output: The video image I' of size mxn.

- Separate Red (R), Green (G) and Blue (B) channels from the video I of size m x n
- Apply one-level DWT on B channel to produce the subband coefficients {LL, LH, H L, H H} of the size m/2 x n/2.
- Apply SVD on the each subband coefficients II = UISIV I to get the singular values AL i = 1,2, ..., n/2, of Sl, l E {LL,LH,HL,HH}
- Apply SVD on watermark W = UwSwVw to get the singular value f', i = 1,2, ..., n/2 of Sw for {LL,LH,Hl,HH} do for 1 to n/2 of ,



- Apply inverse SVD using the singular value i = 1,2, ..., n/2 of l= {LL,LH,HL, HH} to get modified subbands using 1'1 = Ul S' Vl.
- Apply inverse DWT on modified subband coefficients to produce the watermarked B channel.
- Transform the R, G and watermarked B channels into colour image.

Vide Data Hiding Decode

Algorithm in step wise

- The colour image I of size m x n and the monochrome video W of size m/2 × n/2
- Separate Red (R), Green (G) and Blue (B) channels from the colour image I of size m x n
- Apply SVD on the each subband coefficients lI = UISIV I to get the singular values AL i = 1,2, ..., n/2, of Sl, l E {LL,LH,HL,HH}
- Apply SVD on watermark W = UwSwVw to get the singular values Af', i = 1,2, ..., n/2 of Sw

ADVANTAGES

- Attackers cannot find the original data.
- It is not easily cracked.
- To increase the Security.
- To increase the size of stored data.
- Hide more than one bit.

IV. EXPERIMENT AND RESULTS

The proposed method has been implemented using. Java Technology. achievement is the phase of the development when the theoretical design is turned out into a working

system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The achievement phase involve alert preparation, analysis of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of Changeover methods. For more security provides by **SVD.** The SVD is currently one of the favorite public key encryption methods. Here is the algorithm:

4.1 ENCRYPTION TIME

The amount of main time required to execute the encryption algorithm, where the input amount of data depends on the user input is known as the encryption time. The encryption time is also termed as the time complexity of algorithm. The Chart 1 and the table 1 show the encryption time.

Table 4.1 Encryption Time Analysis Table

File Size (MB)	Encryption Time	Encryption /Byte
250	0.25	0.0000125
500	0.23	0.0000128

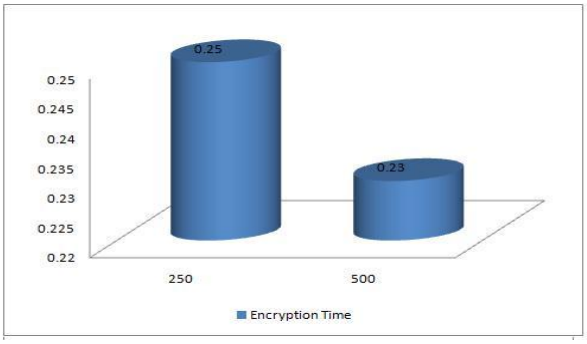


Fig: 4.1 Graphical Representation of the Encryption Time Analysis

4.2 DECRYPTION TIME

For a cryptographic algorithm the amount of main time required, to recover the original text from cipher is explain as decryption time. That can also be termed as space complexity of decryption. The Chart 4.2 and table 4.2 shows amount of time consumed during data recovery. In the diagram X axis shows the different file size used for experimentation and Y axis reports amount of main time consumed.

Table 4.2 Decryption Time Analysis Table

File Size (MB)	Decryption Time	Decryption /Byte
250	0.24	0.0000135
500	0.22	0.0000126

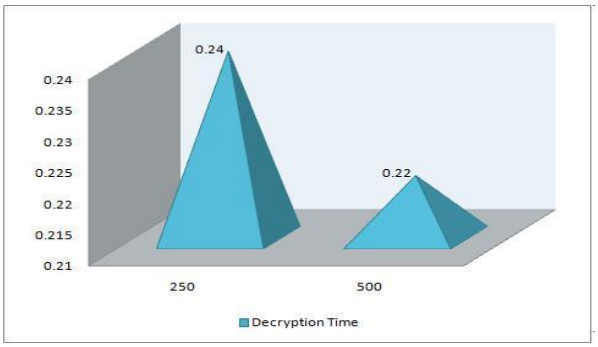


Fig: 4.2 Graphical Representation of the Decryption Time Analysis

IMPLEMENTATION

Authentication

It consists of the username and the password fields. If these fields are valid then only it's possible to view this paper. If these fields are invalid it's prompt out the error message like "Invalid String".

Embedding a message/file in a video file

This module is used to hide message in picture files. Video Location, Save File Location, Encryption Key are provided by the user to hide message in the save file location.

KEY GENERATION

Select x,y	x,y both prime,x=y
Calculate n=x*y	
Calculate $\phi(n)=(x-1)*(y-1)$	
Select integer e	gcd $(\phi(n),e)=1;1<e<\phi(n)$
Calculate d	
Public key	KU={e,n}
Private Key	KR={d,n}

ENCRYPTION

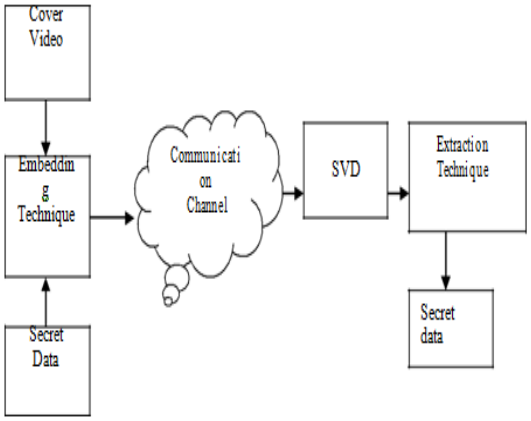
Plaintext:	M<n
Cipher text	$C=M_e \pmod n$

DECRYPTION

Plaintext:	$M=C_d \pmod n$
Cipher text	C

Retrieving the embedded message/file from the video file

This module is used to extract files. Downloaded images by the user are given as input in this text box**.** The key used to extract the file. This is a secret key**.** Receiver should know this key to retrieve message. This is the offset of the file where actually the picture file is resided.



4.1 SYSTEM ARCHITECTURE

Fig 4.1.1 Main Page

Fig 4.1.2 File Data Send

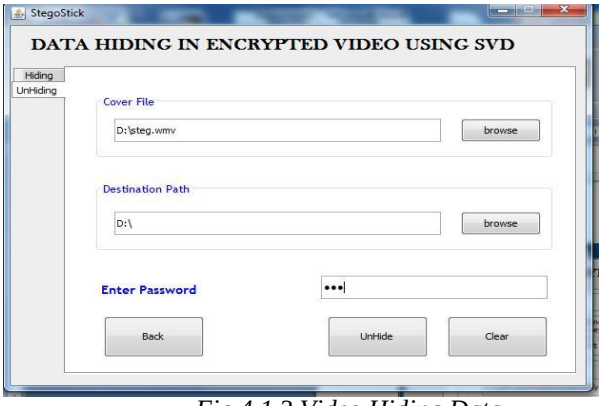


Fig 4.1.3 Video Hiding Data

Fig 4.1.4 Video Extract File download

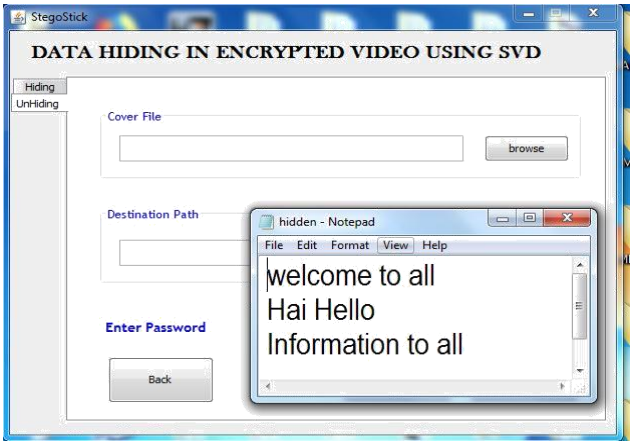


Fig 4.1.5 Message Hiding Video

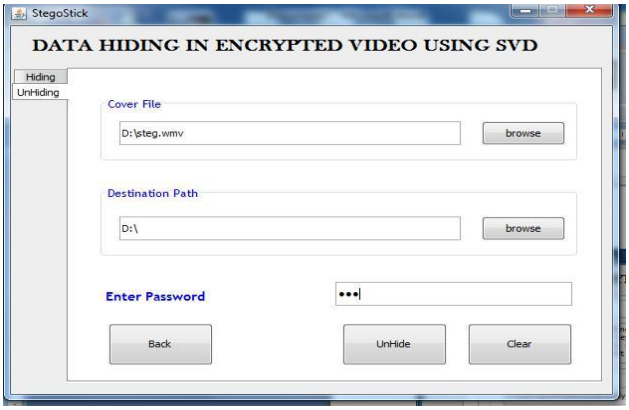


Fig 4.1.6 Message View Hiding Video

Fig 4.1.7 Message View

V. CONCLUSION

A secure video data hiding (VDH) scheme operated over the encrypted domain. A public key modulation mechanism, which allows us to embed the data via simple SVD algorithm, without the need of accessing the secret encryption key. To use a authoritative two-class technique classifier to differentiate encrypt and non-encrypt video patch enable us to both decode the surrounded letter and the original case signal perfectly.

REFERENCES

[1] Noise models in digital image processing Ajay Kumar Boyat1 and Brijendra Kumar Joshi2-2, April 2015.
[2] A survey on security issues: digital images Srinivas Koppu1, madhuviswanatham-18-06-2016.
[3] A Survey on Separable Reversible Data Hiding in Encrypted Image Ganesh Gunjal- 7, July 2015.
[4] Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation J. W. Zhang-2014.
[5] A Survey on Data Hiding Techniques in Encrypted Images- Minu Lalitha Madhavu- 1, January 2016.
[6] Alexandre H. Paqueta, Rabab K. Ward, Ioannis Pitas, Wavelet packets-Based digital watermarking for image Verification and authentication. Signal Processing.2003.
[7] T. Amornraksa, K. Janthawongwilai. Enhanced images watermarking based on amplitude modulation. Journal Image and Vision Computing.2006.
[8] Haohao song_, songyu yu, xiaokang yang, li song, Chen wang. Contourlet-Based
[9] Han-Min Tsai, Long-WenChang. Secure reversible visible mage watermarking with authentication. J Signal Processing: Image Communication.2010.
[10] YounhoLee, Heeyoul Kim, Yongsu Park. A new data hiding scheme for binary image authentication with small image distortion.J Information Sciences.2009

