Journal of Advances and Scholarly Researches in Allied Education
Vol. XIV, Issue No. 1, October-2017, ISSN 2230-7540

Review on Principal Component Analysis Video Steganography and Cryptography in Computer Forensics

Monika Chawla[1]* Dr. S. K. Mishra[2]

[1] Research Scholar, Shri Venkateshwara University, Uttar Pradesh

[2] Faculty of Computer Science Engineering, Shri Venkateshwara University, Uttar Pradesh

Abstract – Video steganography is the art of information hiding mechanism using multimedia. The purpose of the multimedia is getting enlarged day by day. Face recognition systems are also very useful in many applications such as monitoring system, biometrics and security. Principal Component Analysis (PCA) has also been used in some important applications, especially in pattern detection such as face detection and recognition. In real-time applications, the response time must be as small as possible and security must be at a higher level. Steganography and cryptography in computer forensics.

Key Words – Steganography, Cryptography, Principal Component Analysis, Face Recognition

----------X----------

INTRODUCTION

Video Steganography is a mechanism for hiding multimedia data into a multimedia file. The multimedia data which is to be embedded into another file is referred to as a plain data or a message and the multimedia file which is used to hide the message is referred to as cover of the plain data. In this proposed system Steganography as a tool is utilized for face recognition to improve the security and to enhance identification of similar faces. For that an advanced algorithm has been used along with methodologies like Principal Component Analysis and Signcryption. Signcryption is a unique authentication method to identify a person who accesses a computer system.

CRYPTOGRAPHY

Even though Cryptography and Steganography appear to be the same, the former is a wider area and the later is one of the sub domains of the former. Cryptography allows crypting of some information into one file without knowing others. Although, they are often interrelated processes and first encrypting a message, using any one of the stego-tool to hide, they are more effective in hiding a secret message than either method used perse. Cryptography is the process or skill of conveying a message to someone in a secret manner or deciphering secret writing or ciphers. The actual process of cryptography is explained in Figure 1.1.

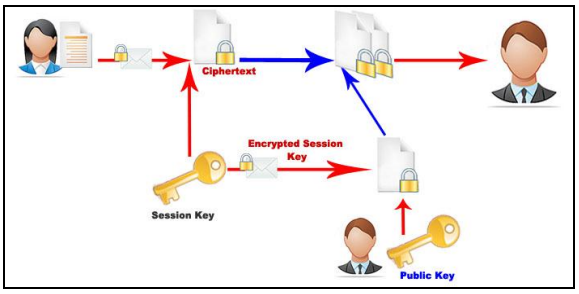

Figure 1.1 Process of cryptography

Plain text is the original message or data that is fed into the algorithm as input.

Encryption is the process that modifies the plain text as cipher text by using any cryptographic algorithm.

Cipher text is the encrypted message that is the combination of the original message and the secret key.

Decryption is the reverse process of encryption is used to get the original plain text using a secret key.

Cryptanalysis is the way to study the methods for gathering original information of the cipher text without using key. It is the study of cracking encryption algorithms or their implementation.

Decryption algorithm takes the cipher text and the secret key to produce original plaintext.

The original raw message, referred to as plaintext, is converted into a random cipher text to conceal the information from unauthorized persons. The original message to be transformed is called the plain text, and the message resulting from the transformation is called the cipher text.

The process of converting a plain text into a cipher text is called encryption. The reverse process is called decryption. The encryption process consists of an algorithm and a key. The key controls the algorithm.

The objective is to design an encryption technique that would be very difficult or impossible for an unauthorized party to decipher the contents of the cipher text. A user can recover the original message only by decrypting the cipher text using the secret key. Depending upon the secret key used, the algorithm will produce different outputs. If the secret key changes, the output of the algorithm also changes.

The security of the conventional encryption depends on several factors. The encryption algorithm should be powerful. Decryption of the message should be difficult. The algorithm is dependent on the secrecy of the key. So, it is mandatory to keep it secret.

Suppose A is the message and encryption key is denoted by k, the encryption process will be written as

B = En (K,A) (1.1)

A = De (K,B) (1.2)

Here B denotes the cipher text. En is a function to encrypt the message A with key K. Decryption De is the inverse process of encryption En

Example: Plain text (X) = This is a sample text, K=strrev(X)

Cipher text (Y) = txet elpmas a si siht

An opponent, observing Y but not having access to K or X, will try to recover X and K. It is assumed that the opponent does have knowledge of the encryption (En) and decryption (De) algorithms.

STEGANOGRAPHY

Steganography is the exercise of concealing valuable information within audio of video file which cannot be seen by normal users. It confuses people because both cryptography and steganography look as similar in the sense that they are used to protect the information. However, steganography is hiding information without knowing others. If anybody tried to see the multimedia with the intention of knowing the hidden data, it cannot be viewed by them.

The statement steganography has a Greek origin. It is a combination of steganos and graptos. 'Steganos' means covered, 'graptos' means writing. It allows concealing a message or any digital information into either audio or video file. It exploits the human perception. Steganalysis is the reverse process of steganography. It tries to detect the concealed data. Figure 1.2 shows the process of steganography.

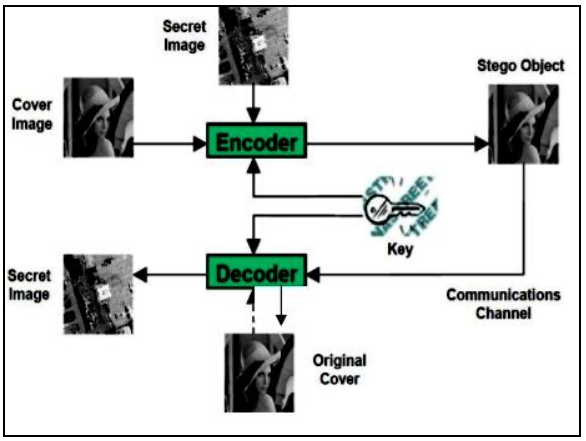

Figure 1.2 Process of steganography

VIDEO STEGANOGRAPHY

Video steganography is one of the versions of steganography among the various types of steganography. In video steganography the input media is a video file. Figure 1.3 shows the process of video steganography.

In Steganography technique we used to transmit a secret message from a sender to a receiver in such a way that only receiver can read the existence message no intermediate person can read the message. In steganography we can hide the information in the form of image, text, audio and video. In old time, we protected data by hiding it on the back of wax and writing tables. Steganography is a security technique for long transmission. To hide secret information or data in images, there are number of steganography techniques in which some are easy while other are complex all of them have their strong and weak points. Image steganography.Provides security when we are sending file over internet. The network security is becoming more important because the number of user exchange the data over internet. We need to protect the data so that unauthorized user can't access it. Mobile banking generally offered account information, transfer, cards and payments etc.

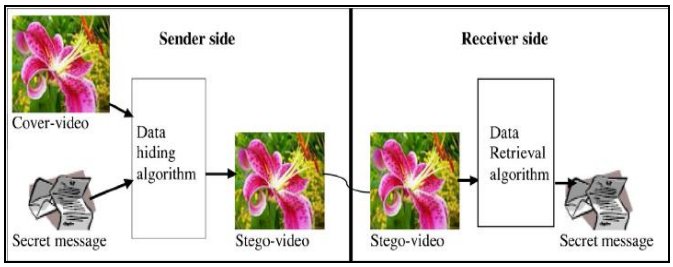

Figure 1.3 Process of Video Steganography

Signature is the original message that is fed into the cover media. Video frames are taken as the cover media.

Key is the way of arranging partitioned digital signature into the cover media.

Encryption is the process of arranging partitioned digital signature into the cover media using any cryptographic algorithm.

Cipher data is the combination of the original message and the secret key.

Decryption is the inverse process of encryption which is used to get original data using secret key. Figures 1.4 and 1.5 show an example of video frames

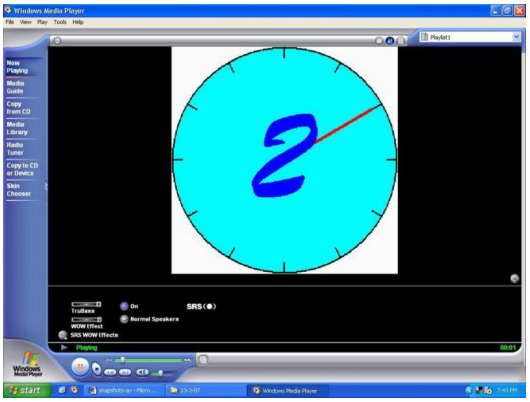

Figure 1.4 AVI file before Steganography - Clock.avi = 81KB

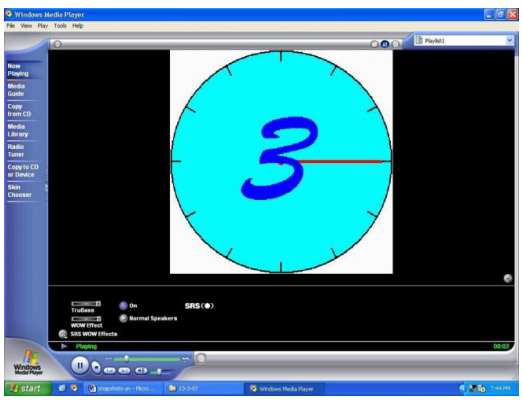

Figure 1.5 AVI file after Steganography Outclock.avi = 81KB (Same size of original)

INDEPENDENT COMPONENT ANALYSIS

Independent component analysis is one of the easiest analysis methods for the domain of artificial intelligence and computer vision. However, it is used to gather the required information from the group of data. It provides a method to conceal data as well as reveal it by its simplified structure. The property of eigen vector decomposition has played a main in it. Let *x* is a data set; *m* is the number of sample. The eigen face method for human face recognition is an information reduction method. Each image can have adequate image information as a Meta data. This information is carefully gathered out of general images to classify the face images. This sub space images have been trained to fix the correct image when a base image is derived, it seems to be found the probed image to match.

The Independent Component Analysis (ICA) is one of the most powerful techniques that have been used in image recognition or face compression. ICA is a statistical method under the broad title of factor analysis. The function of ICA is to reduce the large size of the data space (variables) to the smaller intrinsic dimensionality or size of feature space (independent variables), that are needed to describe the data cost efficiently. This is the case when there is a strong correlation between observed variables.

Since ICA is a classical technique which can perform functions in the linear domain, thus the applications having linear models is much suitable. The field of face recognition is very useful inmany applications such as security, biometric systems, banks and more. Face recognition can be partitioned into Face identification, Face classification, sex determination; people surveillance in crowded areas, video content indexing, and Personal identification used for purposes like Driver's License etc., Mug shots matching and Entrance security.

The main idea of using ICA for face recognition is to express the large 1-D vector of pixels constructed from the 2-D facial image into the compact principal components of the feature space. This can be called as projection of eigenspace.

Eigen space is calculated by identifying the eigenvectors of the covariance matrix derived from a set of facial images (vectors). Once the eigenfaces have been computed, several types of decision can be made depending on the application. Face recognition is a broad term which is categorized as identification where the labels of individuals must be obtained, categorization where the face must be assigned to a certain class.

Recognition of a person, where it must be decided if the individual has already been seen, ICA computes the basis of a space which is represented by its training vectors. These basis vectors, actually

eigenvectors, computed by ICA are in the direction of the largest variance of the training vectors called eigenfaces. Each eigenface can be viewed a feature. When a particular face is projected onto the face space, its vector into the face space describes the importance of each of those features in the face. The face is expressed in the face space by its eigenface coefficients. We can handle a large input vector, facial image, only by taking its small weight vector in the face space. This means that we can reconstruct the original face with some error, since the dimensionality of the image space is much larger than that of face space.

Generally base images are derived for the trained set. Then these trained set are compared with the investigated images. To classify these images Euclidean distance measures have been used.

a. Generation of eigenfaces.

b. Training data is projected into face-space to be used with a predetermined classification method.

c. A projected test element is evaluated by projecting it into face space and comparing to training data.

EARLIER APPROACHES OF FACE RECOGNITION

- **Still Image Face Recognition**

Static image face recognition research is being investigated for the past few decades. Several techiniques are available for image variation between two images. One such is edge mapping. Another is the linear sub space method. Image features are collected according to changes in illumination. However, finding the features of given face image is rather difficult. Adinj et al have investigated that the 20% of misclassification occurred due to illumination changes.

The linear sub space method is followed based upon the convex cone generated by the Convex Lambertain method. A minimum 9 images's needed to construct these convex images. Perfection in the resultant image cannot, however, be assured. This method expects different poses of a human face image.

The equipment has to recognize the given sample face even with different postures or expressions. Morphology method was a technique used to maintain uniformity in all stills with a perfect match not found. The morphed images are used to reveal some features of an image. For example, image of closed eyes is recovered as open eyes of the same person using the texture. The internal part of the eye texture is morphed with the closed eye image.

Various facial expression techniques have been suggested by Liu et al. they have proposed optical flow usage for face recognition. Finding the changes in expression is very difficult in the sub space of given images. The emotions and expressions of a person are known to be unique. The weighing method has been proposed by Martinez et al. to identify various emotions of a specific face. They have devised several sub space components of a given image to find a local sub space and then weigh them separately. However, the features are irresponsive to change an expression rather than being sensitive to lighting.

In Steganography technique we used to transmit a secret message from a sender to a receiver in such a way that only receiver can read the existence message no intermediate person can read the message. In steganography we can hide the information in the form of image, text, audio and video. In old time, we protected data by hiding it on the back of wax and writing tables. Steganography is a security technique for long transmission. To hide secret information or data in images, there are number of steganography techniques in which some are easy while other are complex all of them have their strong and weak points.

Image steganography Provides security when we are sending file over internet. The network security is becoming more important because the number of user exchange the data over internet. We need to protect the data so that unauthorized user can't access it. Mobile banking generally offered account information, transfer, cards and payments etc.

Pose variation is also one of the interesting problems. Wiskott et al have proposed an elastic bunch graph matching method for matching body gesture features. For this purpose, they have used Gabor filter mechanism to extract features. To view several postures of the same image, a multiple view template has been created. Face synthesis is also one of the modern methods to find a specific person's face. Gao et al have built a specific sub area for a given image.

For the past eras, many face recognition systems have been proposed based on principal components analysis (PCA). Even though the particularsare different, all these systems can be described in terms of the same preprocessing and run-time steps. During preprocessing, they register a gallery of ***m*** trained images to each other and unroll each image into a vector of ***n*** pixel values. After that, the mean image for the gallery is subtracted from each and the resulting images are placed in a gallery matrix M. Element [***i; j***] of M is the ***i***th pixel from the ***j***th image.

A covariance matrix Ω=MMT characterizes the distribution of the ***m*** images in Rn. Subsets of the Eigenvectors of Ω are used as the basis vectors for

a subspace in which to compare gallery and novel probe images. When sorted by decreasing Eigen value, the full set of unit length Eigenvectors represents an ortho normal basis where the first direction corresponds to the direction of maximum variance in the images, the second the next largest variance, etc. These basis vectors are the Principle Components of the gallery images.

Once the Eigen space is computed, the centered gallery images are projected into this subspace. At run-time, the recognition is accomplished by projecting a centered probe image into the subspace and the nearest gallery image to the probe image is selected as its match. Here we added signcryption within that probed images for security.

In some systems the images are registered prior to face recognition. Many types of techniques are used to recognize facial features and register them to each other. Different systems may use different distance measures when matching probe images to the nearest gallery image. Different systems select different numbers of Eigenvectors (usually those corresponding to the largest ***k***Eigenvalues) in order to compress the data and to improve accuracy by eliminating Eigenvectors. For helping the people to compare and evaluate, Moon and Phillips created the FERET face database with individual steps of for face recognition process. They also did initial comparisons of some common distance measures. This paper extends their work, by using PCASA.

- **Video-based face recognition**

Video based face recognition also is being developed in modern era. There are several approaches proposed. One is chronological voting. Satoh (2006) has proposed the motionless image matching mechanism. This method follows a distance calculation strategy between two frames of given two videos. The Sequential Importance Sampling (SIS) method has been proposed by Zhou and Chellappa (2002) to obtain time based information. Identity vector with chasing state vector has been used for retrieval of identity details. This is said to be state space model. This model is not suitable if a face is partially blocked.

Zheng and Martinez (2003) proposed probabilistic approach to avoid blurring problem. It encouraged compression algorithm to build time variant features.

A few approaches focusing on spatial features rather than on time variant. Temporal information of video frames has been neglected in this method. In order to produce a specific eigen space, each video frames has been collected and trained to make a person-centric simulation. The distance between the two subspaces is measured by two resemblance videos. Each face is identified by a low dimensional appearance of gathered trained image. Calculation of conversion matrix has been done by the linear probabilistic method. Radial basis models have been developed for small 2D objects. They are not that much suitable for distant poses. Topkaya and Bayazit (2005) have analyzed the dimensional features based on the facial structures.

Another method uses the sparse illustration approach. It is cultured from online databases. A Grey noise covariance matrix is developed using the Principal component Null Space Analysis Method. The Linear Dynamic Model has been used for representing touching measures of the face image. Auto Regressive and Moving Average (ARMA) is the best method for this purpose. Liu and Chen (2011) have proposed the Hidden Markov Model for video based face recognition. Visual representations of facial tracking have also been developed by Kim et al (1996).

All the above methods have some drawbacks while recognizing faces. Facial dynamics is used to differentiate various persons. However, facial expressions and temporal information also have to be registered. Some weights are applied to obtain spatial, temporal information. It is very difficult to assign weights for the dynamically changing video frames. Most of the methods require aligned faces. They need considerable time for verification.

- **Static image and video frames**

Indentification of a person's face by a given video or image is one of the main tasks in face recognition. There are three different possibilities for getting a person's picture, these are: 1. Matching static picture with another static picture, 2. Matching movie with another movie, 3. Matching static picture with movie images.

When the still images have a high quality, good performance can be assured, but video matching is not easy to achieve better performance compared to static image. However, CCTV images does not have clear picture. The noise level is high, the images may be blurred. Maintaining a good resolution of an image is also a challenging task. If the picture has been taken from a very long distance, the resolution will be stumpy. Intermingling with the sub spaces, out of focus of the camera, lighting, motion ratio, pixel clarity are the different factors to find a better solution. Poor factor may lead poor performance and high false rate.

PCA ALGORITHM

The Principal Component Analysis Algorithm is used for the recognition of a human face using eigen vectors. Image M can be represented by a matrix using its pixel values. The vector which is used to represent these values is said to be a eigen values of an image. Sub vectors from these basis vectors to compare stored and acquired new images. Based on

these vectors the principal components of the given image can be found. The acquired new image is then compared with the existing stored images to achieve the perfect match.

Figure 1.6 illustrates the block diagram of PCA.

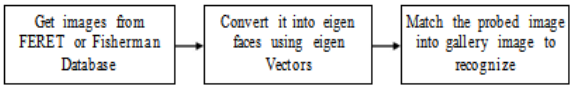

Figure 1.6Block diagram of PCA

CONCLUSION

Steganalysis is the methodology used to find out the embedded data in the stegano images. Brute force is the mechanism to find the key value. It may be tried through a random usage of several combinations of keys. Steganography was in use ancient times. It was used as a method for passing information clandentinely. The motivation for steganography is concealing any digital information without disclosure. It is now used to cloak hidden information in an image or a video or an audio. An earlier method of digital sign has three different functionalities these are: signature gathering, digitalization, and encryption. The problems of these traditional methods are low efficiency and high cost absorption method. The integration cost is also high. Signcryption is a new cryptographic technique that is worth fulfilling those functionalities in a single step.

REFERENCES

1. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt (2008). “Skin tone based steganography in video files exploiting the YcBcR colour space”, ICME 2008, pp. 905-908.

2. Abdi, H., Valentin, D. and Edelman, B. (1998). “Eigen features as intermediate level representations: the case for PCA models”, Brain and Behavioral Sciences, Vol.21, pp. 17-18.

3. Arun Rose, Anil Jain and Sharat Pankanti (1999). “A Prototype Hand Geometry Based Verification System”, 2nd International Conference on Audio and Video Based Person Authentication, Washington D. C., pp. 166-171.

4. Axler, S. (1995). “Linear Algebra Done Right”, Springer-Verlag New York Inc., New York, Second edition.

5. Ayinde, O. and Yang, Y. (2002). “Face recognition approach based on rank correlation of gabor filtered images”, Pattern Recognition, Vol.35, No.6, pp. 1275–1289.

6. B¨auml, M., Bernardin, K., Fischer, M. and Ekenel, H.K. (2010). “Multi-pose face recognition for person retrieval in camera networks”.

7. Balamurugan, V. Mukundhan Srinivasan and Vijayanarayanan, A. (2012). “A New Face Recognition Technique using Gabour Wavelet Transform with Back Propagation Neural Network”, International Journal of Computer Application (IJCA), Vol.49, No.3, pp. 41-46.

8. Baum, L.E., Petrie, T. Soules, G. and Weiss, N. (1970). “A maximization technique occurring in the statistical analysis of probabilistic functions of markov chains”, Ann. Math. Stat., Vol.1, pp. 164–171.

9. Belhumeur, P.N., Hespanha, J.P. and Kriegman, D.J. (1997). “Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.19, pp.711-720.

10. Bentin, S., Allison, T., Puce, A., Perez, E. and McCarthy, G. (1996). “Electrophysiological Studies of Face Perception in Humans”, Journal of Cognitive Neuroscience, Vol.8, No.6, pp. 551-565.

11. Bilmes, J.A. (1998). “A gentle tutorial of the em algorithm and its application to parameter estimation for gaussian mixture and hidden markov models,” Dept. of EECS, U. C. Berkeley, Berkeley, CA 94704, TR-97-021.

12. Blackman, S. and Popoli, R. (1999). “Design and Analysis of Modern Tracking Systems”, Artech House Publishers.

13. Boreki, Guilherm, Zimmer and Alessandro (2005). “Hand Geometry Feature Extraction through Curvature Profile Analysis”, XVIII Brazilian Symposium on Computer Graphics and Image Processing, SIBGRAPI, Brazil.

14. Boreki, Guilherm, Zimmer and Alessandro (2005). “Hand Geometry Feature Extraction through Curvature Profile Analysis”, XVIII Brazilian Symposium on Computer Graphics and Image Processing, SIBGRAPI, Brazil, pp. 149-151.

15. Breiman, L. (1994). “Bagging predictors Technical Report”, Dept. of Statistics, University of California, Berkeley, pp. 421.

16. Bruce, V. and Young, A. (1986). “Understanding Face Recognition”, The

British Journal of Psychology, Vol.77, No.3, pp. 305-327.

17. Brunelli, R. and Poggio, T. (1993). "Face Recognition: Features versus Templates", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.15, No.10, pp. 1042-1052.

Corresponding Author

Monika Chawla*

Research Scholar, Shri Venkateshwara University, Uttar Pradesh