Journal of Advances and Scholarly Researches in Allied Education
Vol. XV, Issue No. 4, June-2018, ISSN 2230-7540

ICASA in Video Steganography

Yamini Pawar[1]* Dr. Abhijit Kumar Pathak[2]

[1] Research Scholar, Maharishi University of Information Technology, Lucknow

[2] Assistant Professor, Maharishi University of Information Technology, Lucknow

Abstract – Video steganography is the craft of data concealing component utilizing multimedia. The reason for the multimedia is getting developed step by step. Face acknowledgment frameworks are additionally valuable in numerous applications, for example, observing framework, biometrics and security. Principal Component Analysis (PCA) has additionally been utilized in some significant applications, particularly in design discovery, for example, face location and acknowledgment. Continuously applications, the reaction time must be as little as could be allowed and security must be at a more significant level. For this reason, another signcryption execution for verifying confirmation by face acknowledgment dependent on the cross-relationship in the frequency area between the information picture and eigen vectors (loads) is proposed. Reproduction results show that the strategy is quicker than the current ones. The trial results for various pictures likewise show great execution. Right now, new face acknowledgment framework utilizing the Independent Component Analysis Signcryption Algorithm (ICASA) inside video steganography is proposed. Relative investigation has likewise been made with the current calculations.

Key Words: Video Steganography, Independent Component Analysis Signcryption Algorithm, Principal Component Analysis

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

1. 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. The proposed method was compared with the existing algorithms to assess the efficiency of our system. The experimental results with the different algorithm and different file formats showed a better performance. As an improvement, in this system a new recognition system using PCASA within Video Steganography is used.

Steganography is an art work to conceal the data into a multimedia file. The purpose of using a multimedia file after than any other file is to accommodate a huge amount of information. A Steganographic system is said to be perfect when both the files which are used to conceal data are the same as in quantity, looks and behaviours. In quantity level and look wise the

Steganographic system can prove to be a perfect secure. To achieve this goal, we proposed PCASA. Research results indicate that the existing systems are giving small corruptions after embedding the data into the file. The proposed system aims to give a clear picture after encryption and decryption.

A multimedia will have some unseen modifications while it allows some data to be embedded in it. Usually data hiding can be divided into two parts, namely, frequency domain and spatial domain. In spatial domain variations in between few pixels can be seen. This method is quite secure but the bit rate is very low. The rate of bit transformations can be increased while segmenting the image. Conjunction with spread spectrum is one method, while exchanging the value of pixels is another. The disadvantage of this method can lead to a very low bit rate when large chip rates are used.

Fast Fourier Transform and Discrete cosine Transform are the frequency domain of image which used to alter the co-efficient of the image. The advantage of frequency domain is that it allows the addition of imperceptible data at a higher rate level. It spreads the data across the full image. It

accepts the compression while trying to add more data in it. However compression in picture may cause a loss of data. Proposed system provides a technique of junk replacement to avoid loss of the original cover media.

During the past few decades, many face recognition systems had been developed on PCA. Although the details vary, they were generally using a set of images for pre processing in a stored data base which has been denoted by *m*. These trained images are matched with another new image as represented as *n* vector by its pixel values. Then the mean value of both the images was produced. Later it was stored under the database.

Image M can be represented by a matrix using its pixel values. A small group of the eigen vectors of is utilized as the basis vector value for a subspace in which to match existing stored images and newly retrieved images. The vector which is used to represent these values is said to be a eigen values of an image. It is called eigen vectors. Covariance matrix is calculated as = MM^T. It characterises the spread eigen values of an image. Sub vectors can be derived from these basis vectors for comparing 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.

A covariance grid recovers the characteristics of the appropriation of the m pictures in n. An internal gathering of the eigen vectors of is utilized as the premise vector for a subspace in which to analyze put away and recently recovered pictures. At the point when arranged by diminishing eigen esteems, the full arrangement of unit length eigen vectors speaks to an ortho-typical premise where the principal heading relates to the bearing of most extreme difference in the pictures, the second the following biggest fluctuation, and so forth. These premise vectors are the Principal Components of the put away pictures. Once the eigenspace is registered, the focused put away pictures are anticipated into this subspace. At the execution time, acknowledgment is satisfied by anticipating a centerly recovered picture into the subspace and the closest put away picture to the new picture is chosen as its match.

There are numerous purposes of distinction among the current frameworks. Some expect that the pictures are enrolled preceding face acknowledgment among the rest, while an assortment of methods are utilized to recognize facial highlights and register them to each other. Various frameworks may utilize distinctive separation estimates when coordinating test pictures to the closest put away picture one. Various frameworks select various quantities of eigen vectors. Those comparing to the biggest k eigen esteems are generally taken with a view to pack the information and to improve precision by taking out eigen vectors. To help assess and look at singular strides of the face acknowledgment procedure, Moon and Phillips (1998) have made the FERET (Facial Recognition Technology) face database, and performed beginning examinations of some basic separation measures. The present work broadens their work, introducing further examinations of separation quantifies over the ongoing prepared arrangement of pictures, videos and analyzing an elective method for choosing subsets of eigen vectors by producing stego pictures and signcryption.

In Data stowing away in sound sign, video signal content and JPEG Images: In this paper the creator presented a vigorous technique for impalpable book, sound, video and picture covering up. They give a productive technique to concealing the information from programmers and it will sent to the recipient in a sheltered way. Along these lines we realize that information concealing systems in sound, this can be utilized for number of purposes other than incognito correspondence.

2. METHODOLOGY

The proposed system used is ICASA (Independent Component Analysis with Signcryption Algorithm). It has the features of ICA and signcryption. At the same time, proposed methodology can reduce the demerits of existing ones. Independent Component Analysis captures the primitive features of the user's face using eigen vectors. Signcryption increase the security of the system. It is discussed in the following Chapters. There are ten important steps:

1. Capturing video.
2. Storing video frames.
3. Getting signature of the user.
4. Application of ICASA:

a. Generation of eigen faces.

b. Implemention of signcryption.

c. Generation of trained set of images.

3. VIDEO STEGANOGRAPHY

Video steganography is one of the variants of steganography among the different kinds of steganography. In video steganography the information media is a video record. Figure 1.3 shows the procedure of video steganography.

In Steganography method we used to transmit a mystery message from a sender to a collector so that no one but recipient can peruse the presence message no middle individual can peruse the

message. In steganography we can shroud the data as picture, content, sound and video. In bygone era, we ensured information by concealing it on the rear of wax and composing tables. Steganography is a security method for long transmission. To shroud mystery data or information in pictures, there are number of steganography procedures in which some are simple while other are mind boggling every one of them have their solid and feeble focuses. Picture steganography.Provides security when we are sending document over web. The system security is turning out to be increasingly significant on the grounds that the quantity of client trade the information over web. We have to ensure the information so unapproved client can't get to it. Versatile banking by and large offered record data, move, cards and installments and so on.

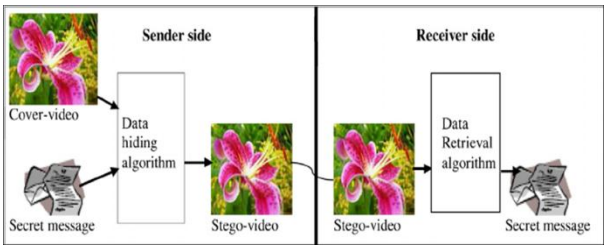

Figure 1.1 Process of Video Steganography

Mark is the first message that is nourished into the spread media. Video outlines are taken as the spread media. Key is the method for organizing parceled advanced mark into the spread media.

Encryption is the way toward organizing divided computerized signature into the spread media utilizing any cryptographic calculation. Figure information is the mix of the first message and the mystery key.

Unscrambling is the converse procedure of encryption which is utilized to get unique information utilizing mystery key. Figures 1.2 and 1.3 show a case of video outlines.

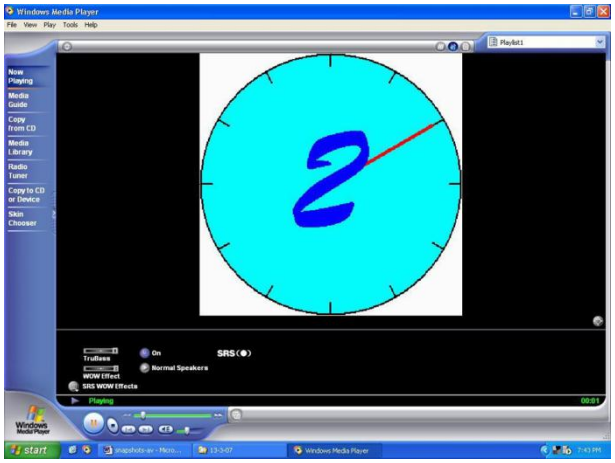

Figure 1.2 AVI file before Steganography - Clock.avi = 81KB

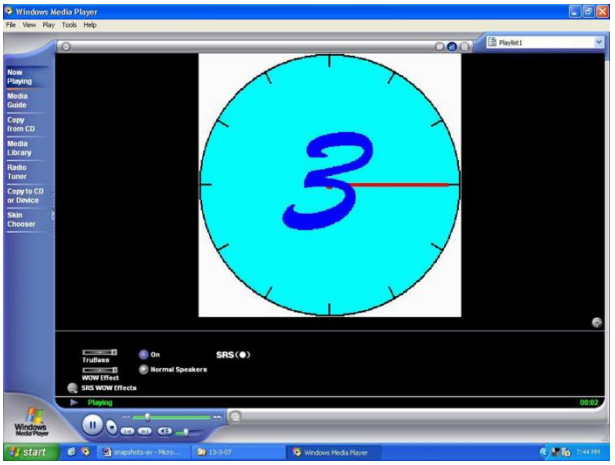

Figure 1.3 AVI file after Steganography Outclock.avi = 81KB (Same size of original)

4. ICASA SYSTEM ARCHITECTURE

► ARCHITECTURE OF ICASA

There are nine important stages.

1. Capture of video
2. Face detection
3. Collection of different postures of face
4. Test signcrypted images when face is already exists
5. Comparison with existing image
6. Features extraction
7. Eigen faces
8. Nearest eigen classifiers
9. Reorganization

Autonomous Component Analysis (ICA). PCA considered picture components as irregular factors with Gaussian appropriation and limited second-request measurements. Unmistakably, for any non-Gaussian conveyance, biggest differences would not relate to PCA premise vectors. Autonomous Component Analysis (ICA) limits both second-request and higherorder conditions in the information and endeavors to discover the premise along which the information (when anticipated onto them) are factually free. Here provided two architectures of ICA for face recognition task: Architecture I – statistically independent basis images (ICA1 in our experiments) and Architecture II – factorial code representation (ICA2 in our experiments), with an addition of signcryption algorithm.

► **IMAGE PROCESSING IN ICASA**

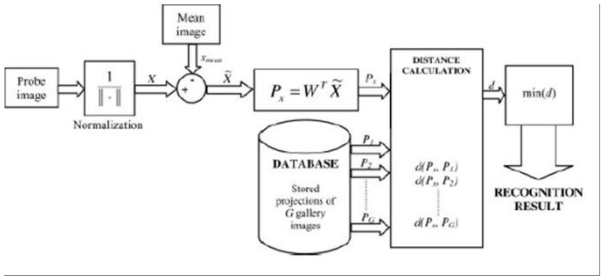

Figure 1.4: **The matching phase of a general subspace face recognition system.**

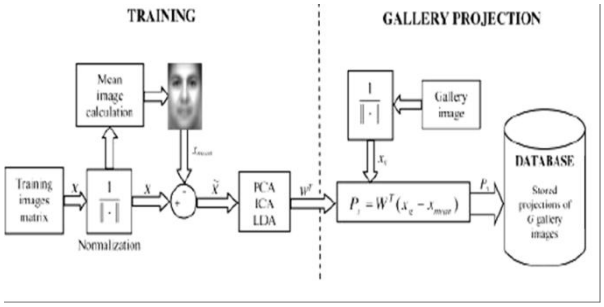

Figure 1.1 Process of Video Steganography

Use case diagram explores the functions of the system and the variety of users of the system. The main components of the use case diagram:

1. Actor: It represents the variety of users of the system. Classifications of the actors are primary, secondary, off-stage.

a. Primary actor – The person who demands the service of the system is considered as the primary actor.

b. Secondary actor – is the provider of the service directly to the customer or user.

c. Off-stage actor – is the person or system who acts as an intermediary in between the service request actor, the service provider actor to do the background process.

d. Supportive actor – Any additional actor used to do the service, is considered as the supportive actor.

In the system, profounded in this research work, users are considered as the primary actors to get the service from the system. ICASA system is considered as the secondary actor. The signature recognizer is the supportive actor. The encryption system is the off-stage actor. A major issue in neural system look into, just as in numerous different controls, is finding a suitablerepresentation of multivariate information, for example arbitrary vectors. For reasons of computational and applied straightforwardness, the portrayal is regularly looked for as a direct change of the first information.

As such, every component of the portrayal is a direct blend of the first factors. Notable direct change techniques incorporate principal component examination, factor investigation, and projection interest. Free component examination syncryption calculation (ICASA) is a rdeveloped technique in which the objective is to locate a straight portrayal of nongaussian information with the goal that the components are measurably autonomous, or as free as could be expected under the circumstances.

2. Use cases: Use cases are the text which depicts the common services of the system.

The role of each actor is:

User (primary actor) – request entry of the service of the system.

ICASA (secondary actor) – provides the service for recognition of the right user.

Signature recognizer (supportive actor) – receives the user's signature. Encryption system (off-stage actor) – encrypts the data.

Six use cases are derived from Figure 3.2. They are:

1. Login – is the process that is used by the user to enter into the system by giving their data.

2. Capture video – is the process for getting the face posture of the user; system automatically will take the video clip.

3. Get sign – is the process of the system that requests the signature from the user.

4. Match data – is the process of the system for checking the new input with the existing one.

5. Provide DSC – is the process which when given data match, generates Dynamic Secret Code (DSC).

6. Update trained set – This is the process wherein, whenever a user enters into the system, the system will update the different face postures.

5. CONCLUSION

Each and every image can have the color mode property which can hold a number of colors in the image file. Achievement of desirable quality needs chance of a high colour mode. The range of the color mode can be 2 X 256 colors. It is suitable for simple graphics and drawings. High color modes can use more than 256 colors. Photos and images used a high color mode with color palette, which

uses RGB color space. So each and every pixel may hold the intensity value of Red, Green, Blue (RGB). JPEG does not support color palette but the result is excellent one. PNG supports upto 256 tera colors. Now-a-days common desktop computers used more than 16 million colors.

GIF file format supports low color modes. It is not that much suitable for high color mode photos.

Storage of the attribute values of an image or photo is easier in gray scale mode than a high color mode. The reason is that monochrome pictures needs only two value but color modes needs more. Black & White (B&W) mode images are entirely different from 2-color mode images. Even though number of intensity value of B&W images and 2-color images are the same, 2-color images can use any two colors. Portable Network Graphics (PNG) files are capable to store both gray scale and B&W.

The intensity of the pixel color is achieved by its depth of the pixel value. It represents the number of bits required to glow a pixel. The formula Colors = $2^{bitdepth}$ is used to determine the number of different shades of an image.

Interpretation of a media object is necessary as those objects are unstructured and need to be a binary format. Interpretation of those objects into a machine readable format needs meta data of an object. The meta data is nothing but data about data. It contains the detail information about the multimedia object. The meta data can be extracted from either intra media or inter media. Intra media contains the information within an object but inter media having all other media details with its relationship under one function.

Mode of interpretation can be done automatically or semi automatically or manually. The function which is used to extract the features of an object is said to be extracting functions. Inter media has only function but inter media has n number of functions for n number of objects. There are three types of meta data, i) Content related meta data, ii) Content expressive meta data and iii) Content deviated meta data.

Content related meta data: It contains the information about its content. For an example facial features may contain skin color, hair color, size of the nose, ear and eye.

Content expressive meta data: It deals with object information with the help of the user's data. Example: Meta data on facial expression such as smile, sadness, happiness. It needs the content of image as well as the additional cognitive information of the system.

Content deviated meta data: It contains content deviated information but that information may merely not be associated with the content. For example, name of the photographer, director of the movie, etc.

Meta data generation methodologies: Feature extraction of an image can be employed by any one of these content-dependent or content expressive methodologies. The terminologies which are used to represent an application's view and its object content are referred by ontologies. These terminologies create a semantic space to map with its meta data. Some of the ontologies used to derive the meta data of an (image) object.

Media dependent ontologies: it is interrelated with its concepts and relationships, example audio-volume, video-colors, media independent ontologies. These ontologies describe the independent characteristics of the media objects such as location, owner name.

Meta correlations: it is related with different type of media objects to explore the relationships among them. It frames a unified picture of a multimedia data base, and is called by query meta data. This meta data is used to fulfill the needs of data base to derive application-based ontologies.

Example: query on geographic information, those states are heavy rained and coastal areas with natural harbours.

Meta data of video sequences can be stored in a single frame or multiple frames of which, there are three:

i) Content related meta data

ii) Content expressive meta data

iii) Content independent meta data

i) Content related: It includes nature of the camera like: As titling camera, zooming camera, panning camera and color level of the object, nature of the object. Single frame meta data hold the histogram information of the pixel colors.

ii) Content expressive: It may have details about the content such as distance between the object and camera, action description, type of objects, etc. In a single frame meta data can hold the same additionally texture, color of the object.

iii) Content deviated: It holds the details about the whole video. Extraction of this information from the content related meta data needs some extraction algorithm to divide the video frames. The nature of the content-deviated meta data is it does not have the details of the raw content. Hence

user or a system needs to be given those details.

REFRENCES

ICME 2008, Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt (2008). "Skin tone based steganography in YcBcR color space video files." pp. 905-908,

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.

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

Balamurugan, V. Mukundhan Srinivasan andVijayanarayanan, 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, July 2012.

Chang, M.C., Krahnstoever, N., Lim, S. and Yu, T. (2010). “Group level activity recognition in crowded environments across multiple cameras in AMMCSS”, pp. 56-63.

A.P., Dempster, Laird, N.M. Rubin, D. B. (1977). "Maximum likelihood through the em algorithm with incomplete data," Royal Statistical Society Journal: Series B, Vol.39, No.1, pp.1–38.

Corresponding Author

Yamini Pawar*

Research Scholar, Maharishi University of Information Technology, Lucknow