Journal of Advances and Scholarly Researches in Allied Education
Vol. 15, Issue No. 11, November-2018, ISSN 2230-7540

An Experimental Analysis on Independent Component Analysis Signcryption Algorithm Video Steganography

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. 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. The experimental results for different images also show good performance. In this thesis, a new face recognition system using the Independent Component Analysis Signcryption Algorithm (ICASA) within video steganography is proposed.

Key Words – Steganography, Signcryption, ICASA, 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. 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

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 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.

SIGNCRYPTION

Signcryption is one of cryptography methods which can perform the functions of both digital unique user signature and encryption. These tools can ensure the primary properties of information security such as confidentiality, integrity and reducing redundancy. In Data hiding in audio signal, video signal text and JPEG Images: In this paper the author introduced a robust method of imperceptible text, audio, video and image hiding. They provide an efficient method for hiding the data

from hackers and it will sent to the receiver in a safe manner.

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. It reduces the computational costs and solves communication problems. The normal signcryption method uses a single session key which is reusable for several encryption methods. The problem of the single session key causes low security when a plain text model is chosen. This is the reason for choosing a random session key for a hybrid encryption scheme.

ARCHITECTURE OF ICASA

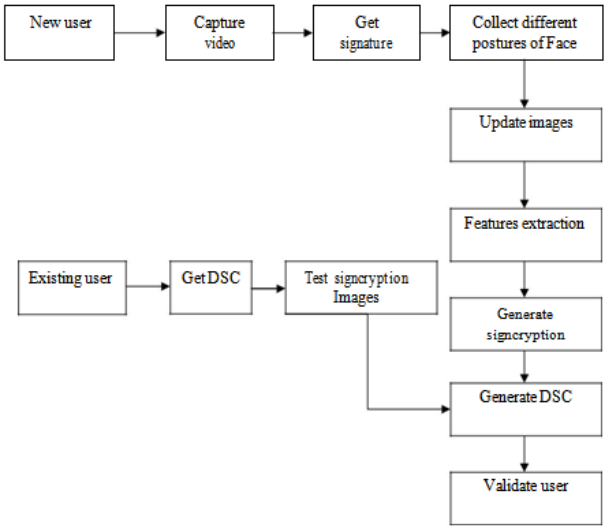

Figure 1 Block diagram of ICASA

Figure 3.1 illustrates the block diagram 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

Independent Component Analysis (ICA). PCA considered image elements as random variables with Gaussian distribution and minimized second-order statistics. Clearly, for any non-Gaussian distribution, largest variances would not correspond to PCA basis vectors. Independent Component Analysis (ICA) minimizes both second-order and higherorder dependencies in the input data and attempts to find the basis along which the data (when projected onto them) are statistically independent. 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

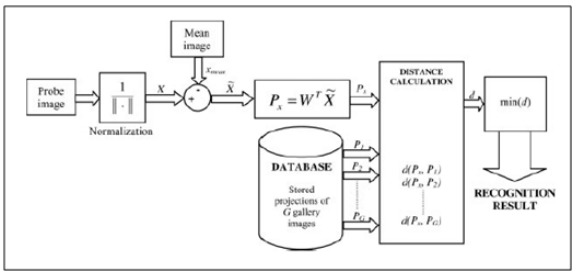

Figure 2: **The matching phase of a general subspace face recognition system**

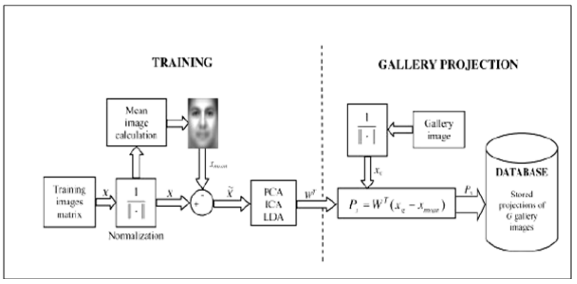

Figure 3: An illustration of general subspace appearance-based face recognition system

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 fundamental problem in neural network research, as well as in many other disciplines, is finding a suitable representation of multivariate data, i.e. random vectors. For reasons of computational and conceptual simplicity, the representation is often sought as a linear transformation of the original data.

In other words, each component of the representation is a linear combination of the original variables. Well-known linear transformation methods include principal component analysis, factor analysis, and projection pursuit. Independent component analysis syncryption algorithm (ICASA) is a redeveloped method in which the goal is to find a linear representation of nongaussian data so that the components are statistically independent, or as independent as possible.

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 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.

CLASS DIAGRAM

Class diagrams forms the domain models of the system. It explores the entire structure of the system. More than that, class diagrams derive the relationship or association in between their interfaces. This denotes the logical view of the system.

Components of the class diagrams are

i) Classes – Real time group of objects.

ii) Aggregations – Collection of classes under one group.

iii) Generalization – General group name of combined sub groups.

iv) Specialization-Special group name of specific sub groups.

v) Inheritance-Relaying the attributes and behavior to its sub classes.

vi) Cardinality – Number of connectivity in the cardinal way.

vii) Modality - Availability of connectivity.

viii) Multiplicity - Number of connectivities belongs to its classes.

ix) Role name - Name of the behavior.

x) Attributes - Qualities in nature.

xi) Functions – Methods to do its works.

xii) Accessibility – Mode of visibility and retrieval authenticity.

a) Classes and their structure and behavior – Class names are indicated at the top of the class diagram as users, video, and sign. Each rectangle box indicates the attributes and behavior of the class. It has three compartments. The top compartment indicates the name of the class or object. The middle compartment indicates characteristics, qualities, attributes of the class. The bottom compartment indicates the functionalities of the class.

b) Association, aggregation, dependency and inheritance relationships – Relationships between the classes are indicated by arrows. If more than one class is needed for connection with another class, the middle agent is considered as association class.

Aggregation allows a combination of several classes.

Figure 3 shows the dependency between the classes by messages over an arrow. Multiple and multi-level inheritance can also be denoted by hollow arrows.

c) Multiplicity and navigation indicators – Multiplicity is one of the characteristics of the class diagram used to denote the number of relationships. Navigation indicators are used to indicate the directions of the message passing by arrow.

d) Role names – Most of the class names are created by the role names.

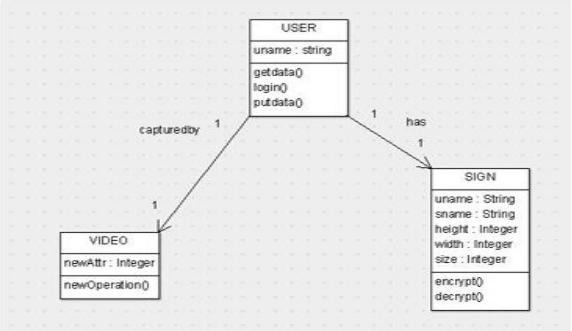

Figure 4 Class diagram1

Figure 3 illustrates relationship between user, video and sign.

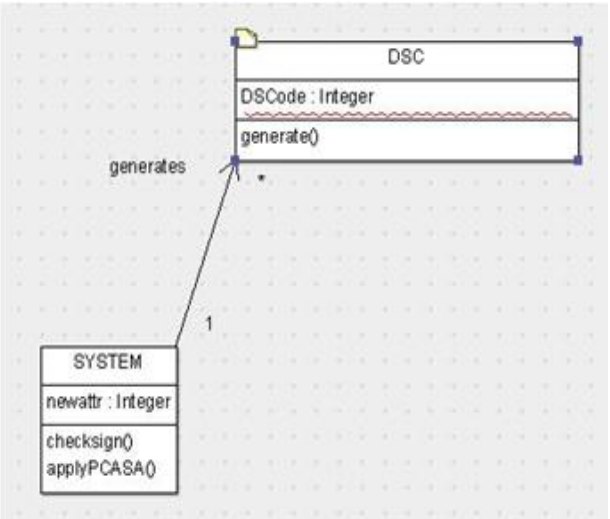

Figure 5 Class diagram2

Figures 3and 4 illustrate the attributes and functions of the objects.

ACTIVITY DIAGRAM

The activity diagram determines the internal activities of the system and its behavior. Components of the activity diagrams are:

Swim lanes: They assign the proper path of space for the objects by dividing such objects over lines.

States of the action: Represent the actions of the entities as in the system flow steps.

Action flows: The flow of actions is represented by arrows with its respective responsibilities.

Object flows: It controls the action states.

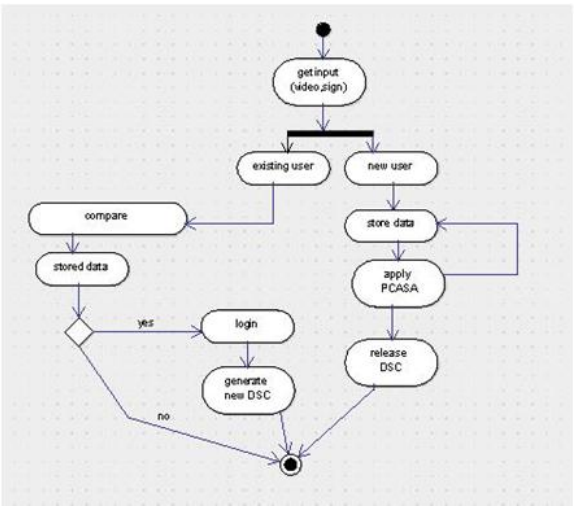

Figure 6 Activity diagram

Figure 6 illustrates the entire range of activities of the PCASA system. The filled circle represents the start of the process. The rounded rectangle symbol represents activities. The diagonal symbol represents decision making conditional statements. The solid arrows represent the flow of the process. Rounded filled circle represents that the activities are halted.

SEQUENCE DIAGRAM

The sequence diagram is used to pass the messages in between two classes or objects. It mainly concentrates on classes and the inter communication of its works by message passing.

- These diagrams focus on classes and the messages they exchange to accomplish some desired behavior.
- Sequence diagrams are a type of interaction diagrams. They have the following components:

Class roles: Represents play roles of an object.

Lifelines: Represent the availability existence of an object over a period of time.

Activation: Represent the time during which an object is performing an operation.

Messages: Represent communication between objects.

Scenario 1: If a new user comes to register

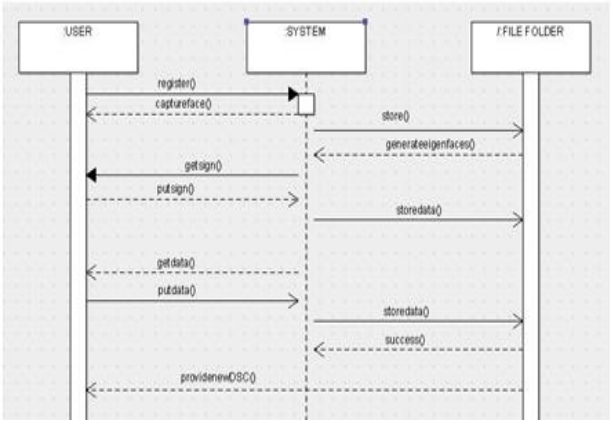

Figure 7 Sequence diagram - Scenario 1

Scenario 2: If existing user comes

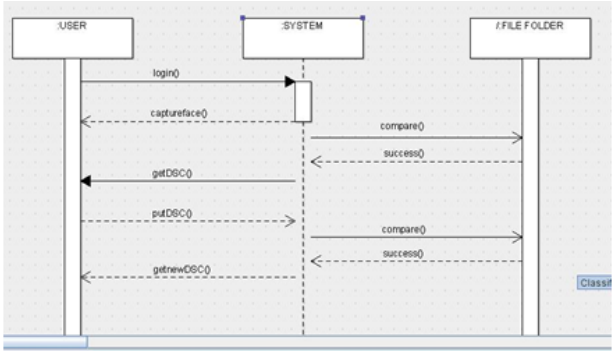

Figure 8. Sequence diagram – Scenario 2

Figure 7 explains the scenario of a new user entering the system. Figure 8 explains the scenario of an existing system user's log in. Figure 9 illustrates the activity when the same user comes in but in a different style. Figure 10 illustrates the activity when an entirely different user looks like the existing one. The sequence diagram demonstrates the interactions between the user and the system. Rectangle boxes are represented by the objects. The solid arrow which carries message from left to right request the service to the system. Dotted arrow represents responses from the system. Messages are explained by the functions of each object.

Scenario 3: Same user with different clothing

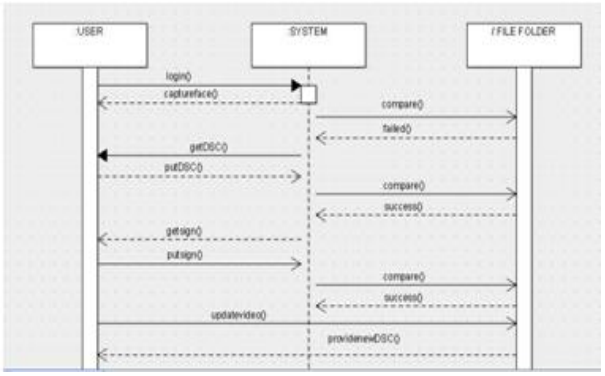

Figure 9 Sequence diagram - Scenario 3

Scenario 4: If different user, looking as existing one

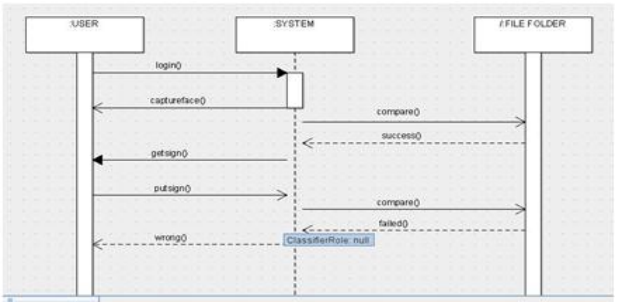

Figure 10 Sequence diagram - Scenario 4

CREATING SIGNCRYPTED IMAGES

In order to enhance the security of the system proposed, the system enables signcryption for the given user's data. PCASA generates the signcrypted images. The given signature is fragmented into several parts and is stored into the eigen faces. Then, the system will generate the DSC. The following sections illustrate signcryption on video steganography. To create signcrypted images, following steps are carried out by the PCASA system.

Generation of signature image

In order to manipulate the signcrypted image, we need a sample signature of the user. Figure 11 shows the sample user's signatures. To get user signature, system needs drawing tablet.

Figure 11 Sample input signature

Fragmentation of signature image

Figure 12 Fragmented signature image

Figure 12 shows the fragmented signature images of given input image as shown in Figure 13. This input image has been cropped into four parts shown as Figures 14, 15, 16and 17.

Figure 13 Input image

Figure 14 Part 1

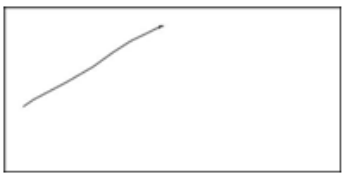

Figure 15 Part 2

Figure 16 Part 3

Figure 17 part 4

Signature image has been fragmented into several parts by ICASA at the first time as shown in Figures 14 through 17.

Signcryption of signature image

The scrambled parts of the signature have been embedded into existing captured images using ICASA. Hereafter, it will be called as signcrypted image.

Figure 18 Signcrypted images

Figure 18 shows the signcrypted image. Fragmented signature has been stored into corresponding user's video clipping.

Output video

Input and output files are look as same. There is no variation in between the file size.

Figure 19 Before video steganography (3.66MB)

Figure 20 After video steganography (3.66MB)

Figures 19 and 20 show the sample input, output video clippings. These are looking as identical. However, persons with technical knowledge will

know they are not. Figure 20 has been used to identify the user for his/her next log in.

CONCLUSION

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. The experimental results of the proposed system which we get from ICASA. Thus, the user has been identified using ICASA successfully without any distortion on the picture. Resultant output shows that the file size of both input and output are same. Thus the research work has been done to achieve a secure and unique face recognition system by innovative way of using signcryption and video steganography.

REFERENCES

[1]. Moon, H. and Phillips, J. (1998). "Analysis of PCA-based face recognition algorithms", Empirical Evaluation Techniques in Computer Vision, IEEE Computer Society Press, pp. 588.

[2]. Mukundhan, Srinivasan and Vijayanarayanan, A. (2012). "Independent Component Analysis of Edge Information for Face Recognition under Variation of Pose and Illumination", in Proceedings of Fourth International Conference on Computational Intelligence, Modeling and Simulation (CimSIM2012), pp. 226-231.

[3]. Joachim J., Eggers and B¨auml, R. (2002). "A Communications Approach to Image Steganography, Telecommunications Laboratory", Proceedings of SPIE, Vol.4675, pp. 26-37.

[4]. John, C. and Russ (2007). "Handbook of Image Processing", Taylor & Francis Group, LC, Fifth Edition.

[5]. John Carter and Mark Nixon, "An Integrated Biometric Database", available at: ieeexplore.ieee.org/iel3/1853/4826/00190224.pdf.

[6]. Johnson, N.F. and Jajodia, S. (1998). "Exploring steganography: seeing the unseen", IEEE Computer, Vol.31, No.2, pp. 26–34.

[7]. Jolliffe, I.T. (1986). "Principal component analysis", Springer series in statistics, ISSN 0172-7397, Springer-Verlag.

[8]. Jonathon Shlens (2005). "A Tutorial on Principal Component Analysis Systems", Neurobiology Laboratory, Salk Insitute for Biological Studies La Jolla, (Version 2), 2005.

[9]. Kanade, T. (1973). "Picture Processing by Computer Complex and Recognition of Human Faces", Technical report, Dept. Information Science, Kyoto University.

[10]. Hao-Bin, Zhao Li-Yi and Zhong Wei-Dong (2011). "A Novel Steganography Algorithm Based on Motion Vector and Matrix Encoding", IEEE Transactions, pp.406-409.

[11]. James R. Parker and Parker, J.R. (1996). "Algorithms for Image Processing and Computer Vision", John Wiley & Sons.

[12]. Jay Devore and Roxy Peck (1997). "Statistics: The Exploration and Analysis of Data", Brooks Cole, Third Edition.

[13]. Joachim J., Eggers and B¨auml, R. (2002). "A Communications Approach to Image Steganography, Telecommunications Laboratory", Proceedings of SPIE, Vol. 4675, pp. 26-37.

[14]. John, C. and Russ (2007). "Handbook of Image Processing", Taylor & Francis Group, LLC, Fifth Edition.

[15]. John Carter and Mark Nixon, "An Integrated Biometric Database", available at: ieeexplore.ieee.org/iel3/1853/4826/00190224.pdf.

[16]. Johnson, N.F. and Jajodia, S. (1998). "Exploring steganography: seeing the unseen", IEEE Computer, Vol. 31, No. 2, pp. 26–34.

Corresponding Author

Monika Chawla*

Research Scholar, Shri Venkateshwara University, Uttar Pradesh