An Overview to Cryptography and Its Aspects

Mr.Azharuddin Allamin Shaikh is currently pursuing degree program in electronics and telecommunication engineering in SHIVAJI University, India,

Mr. Abidali G. Surati is currently working as Assistant professor in electronics and telecommunication engineering in
Annasaheb Dange College Of Engg. And Technology, Ashta. In SHIVAJI University, India,

Mr. Ritesh Anant Jadhav is currently working as Assistant professor in electronics and telecommunication engineering in Annasaheb Dange College Of Engg. And Technology, Ashta. In SHIVAJI University, India,

Mr. Harshad Daingade is currently working as Assistant professor in electronics and telecommunication engineering in
Annasaheb Dange College Of Engg. And Technology, Ashta. In SHIVAJI University, India,

IJERT

Abstract - IN day today life it has become important to be secured , hence cryptography is an technique provides certain needs by its application in visual (image ,video ,text ,etc.).in this paper we are trying to focus on some of its application which are really for human welfare. IN This paper Specifically we would like to elaborate our experience on the significance of human detection by ear biometric , face recognition ,digital signatures and other related emerging application of cryptography.

Index Terms- cryptography , Steganography , ear biometrics, face detection and recognition, digital signature , Moni Naor and Adi Shamir etc .

1. INTRODUCTION

Visual Cryptography is an art of hiding the information in secure manner which can be regained by means of breaking it in parts (share) , it allows visual information such as picture , text ,video , etc. the foundation of cryptography was laid by Moni Naor and Adi Shamir in 1994 . The importance of embedded applications on image and video processing, communication and cryptography domain has been taking a larger space in current research era hence it is becoming a inseparable part. On the other side Image processing is a technique to perform an algorithmic strategy to signaling an image in

multidimensional .systematic way The main objective of our paper is to use this technology for a new level of image processing technique to ensure its most convincing level of encrypt and decrypt data using Visual Cryptography Schemes. Cryptography is well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in their Computer science and other related fields: they are used to protect e-mail messages, credit card information and etc.

2. IMAGE AND VIDEO ENCRYPTION

It has to be decide that either a full encryption or an selective encryption is required according to the application. SE is a technique aiming to reduce the required computational time and to enable new system functionalities by encrypting only a portion of the compressed bit stream while still achieving adequate security. has two main advantages; first, it reduces the computational requirements, since only a part of plaintext is encrypted; second, the encrypted bit stream maintains the essential properties of original bit stream. The encrypted bit stream will be compliant and fulfil*l* real time constraints if the following three conditions are filled:

• To keep the bit rate of encrypted bit stream original bit stream, encrypted code words must have the
same size as the original code words.

• The encrypted code words must be valid so that they may be decoded by entropy decoder.

• The decoded value of syntax element from encrypted code words must stay in the valid range for that syntax element. Any syntax element which is used for prediction of neighboring MBs should not be encrypted. Several SE methods of image and video based on the Advanced Encryption Standard (AES) has been proposed in literature. For example the encryption of color images in the wavelet transform has been addressed , SE was performed on color JPEG images by selectively encrypting only the luma component using the AES cipher.In the field of video, SE of H.264 video is proposed by doing frequency domain selective scrambling, DCT block shufling and rotation . SE of ROI of H.264 has been presented . It performs SE by pseudo-randomly inverting sign of DCT coefficients in ROI. A scheme for commutative encryption and watermarking of H.264/AVC is presented.Here SE of some MB header fields is combined with watermarking of magnitude of DCT coefficients but they are not format compliant. SE scheme based on H.264/AVC has been presented on CAVLC and CABAC for I and P frames .This method fulfills real-time constraints by keeping the same bit rate and by generating a completely compliant bit stream. Perceptual encryption has also been presented in where encryption is done with an alternative transform of the DCT coefficients. The robustness of SE videos to attacks which exploit the information from non-encrypted bits together with the availability of side information was studied in .A new challenge in SE of image and video is to decrease the percentage of encrypted bits by keeping the same confidentiality level

3. Ear Biometrics.

Using cryptography technique we can also recognize humans , as human ears have been used as major feature in the forensic science for many years. Recently so called earprints, found on the crime scene, have been used as a proof in over few hundreds cases in the Netherlands and the United States .

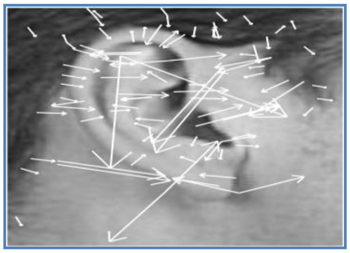

Figure 1

However, still the automated system of ear recognition hasn’t been implemented even though there are many advantages of using ear as a source of data for person identification. Firstly, ear does not change considerably during human life, and face changes more significantly with age than any other part of human body. Face can also change due to cosmetics, facial hair and hair styling. Secondly, face changes due to emotions and expresses different states of mind like sadness, happiness, fear or surprise. In contrast, ear features are relatively fixed and unchangeable . 86 M. Choraś / Electronic Letters on Computer Vision and Image Analysis 5(3):84-95, 2005 Moreover, the colour distribution is more uniform in ear than in human face, iris or retina. Thanks to that fact, not much information is lost while working with the grey scale or binarized images, as we do in our method Figure 2 presents two more aspects of ear identification. Firstly, ear is one of our sensors, therefore it is usually visible (not hidden underneath anything) to enable good hearing. Ear is also smaller than face, which means that it is possible to work faster and more efficiently with the images with the lower resolution.

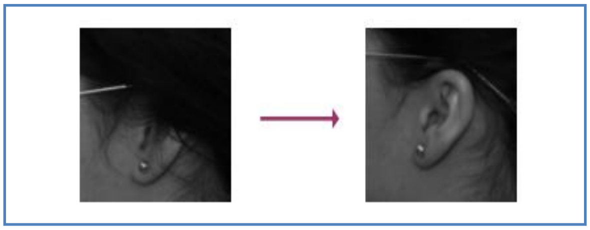

Figure 2 (ear visibility and size)

In the process of acquisition, in contrast to face identification systems, ear images cannot be disturbed by glasses, beard nor make-up. However, occlusion by hair or

IJERT

earrings is possible, but in access control applications, making ear visible is not a problem for user and takes just single seconds (Figure 3). Fig. 3. Ear visibility can be easily achieved in applications allowing interaction with the user (for example access control systems) The first, manual method, used by Iannarelli in the research in which he examined over 10000 ears and proved their uniqueness, was based on measuring the distances between specific points of the ear . The major problem in ear identification systems is discovering automated method to extract those specific, key points. Another well-known method by Burge and Burger was based on building neighborhood graph from Voronoi diagrams of the detected edges. Hurley et al. introduced a method based on energy features of the image. They proposed to perform force field transformation in order to find energy lines, wells and channels. Another method used by Victor at al in the experiment comparing ear and face properties in order to successfully identify humans in various conditions, was based on PCA. Their work proved that ear images are a very suitable source of data for identification and their results for ear images were not significantly different from those achieved for face images. The method, however, was not fully automated, since the reference points had to be manually inserted into images. Another approach presented by Moreno et al was based on macro features extracted by compression networks.

IJERT

4. FACE DETECTION AND RECOGNITION

The image and video data gathered via online photography and video sharing sites, street view, surveillance cameras and institutional databases can easily be used by autonomous systems that use efficient face detection and recognition algorithms to identify and track individuals. This capability raises serious privacy concerns among people. As a result of these concerns, we have witnessed a significant increase in number of privacy related research in the field of face detection and recognition on image and video data in recent year. In the following, we briefly summarize the state-of-the-art that uses cryptographic techniques to address the privacy issues in the field of face detection and recognition .Senior and Pankanti provide a description of privacy and give a brief summary on the privacy protection mechanisms for face recognition systems. Lu *et al* discuss problems and challenges in secure video processing. The solutions based on cryptographic techniques proposed in the literature focus on different techniques like homo morphic encryption (HE), secret sharing and multiparty computation. Avidan and But main propose a face detection algorithm based on machine learning that is particularly designed for realizing the algorithm efficiently by using secure multi party computation. Erkin *et al*. propose to encrypt face images using HE and let the Eigen face recognition algorithm work on encrypted data without revealing private information to the holder of the face database as illustrated in Figure 1. Sade ghi*et* further improve the efficiency of that approach by replacing the matching mechanism with a fine-tuned garbled circuit.

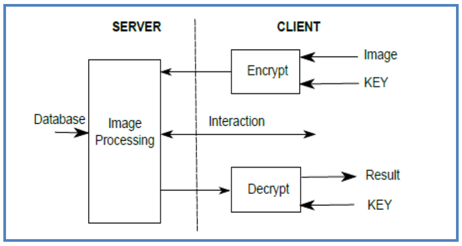

Figure 3

Fig.3. Protocol actions in the secure face recognition system .Existing literature on privacy protection in video processing for surveillance also relies on cryptographic primitives .Upmanu *et al*. use secret sharing that requires distributed secure processing and storage. Sohn *et al*. propose watch list screening for video surveillance systems that discriminates groups of identities of interest without revealing face images. For this purpose, the authors use HE to prevent revealing the private information. Osadchy *et al*. propose a new face identification system that is designed for usage insecure computation based on HE and oblivious transfer protocols.

5. DIGITAL SIGNATURE

Just as handwritten signatures or physical thumbprints are commonly used to uniquely identify people for legal proceedings or transactions, so digital signatures ("digital thumbprints") are commonly used to identify electronic entities for online transactions. A *digital signature* uniquely identifies the originator of digitally signed data and also ensures the integrity of the signed data against tampering or corruption.

One possible method for creating a digital signature is for the originator of data to create the signature by encrypting all of the data with the originator's private key and enclosing the signature with the original data. Anyone with the originator's public key can decrypt the signature and compare the decrypted message to the original message.

Because only someone with the private key can create the signature, the integrity of the message is verified when the decrypted message matches the original. If an intruder alters the original message during transit, the intruder cannot also create a new valid signature. If an intruder alters the signature during transit, the signature does not verify properly and is invalid.

However, encrypting all data to provide a digital signature is impractical for three reasons:

- The ciphertext signature is the same size as the corresponding plaintext, so message sizes are doubled, consuming large amounts of bandwidth and storage space.
- Public key encryption is slow and places heavy computational loads on computer processors, so network and computer performance can be significantly degraded.
- Encrypting the entire contents of information produces large amounts of ciphertext, which can be used for cryptanalysis attacks, especially known plaintext attacks (where certain parts of the encrypted data, such as e-mail headers, are known beforehand to the attacker).

Digital signature algorithms use more efficient methods to create digital signatures. The most common types of digital signatures today are created by signing message digests with the originator's private key to create a digital thumbprint of the data. Because only the message digest is signed, the signature is usually much shorter than the data that was signed. Therefore, digital signatures place a relatively low load on computer processors during the signing process, consume insignificant amounts of bandwidth, and produce small amounts of ciphertext for cryptanalysis. Two of the most widely used digital signature algorithms today are the RSA digital signature process and the Digital Signature Algorithm (DSA).

RSA Data Security Digital Signature Process

In the RSA digital signature process, the private key is used to encrypt only the message digest. The encrypted message digest becomes the digital signature and is attached to the original data. Figure illustrates the basic RSA Data Security digital signature process

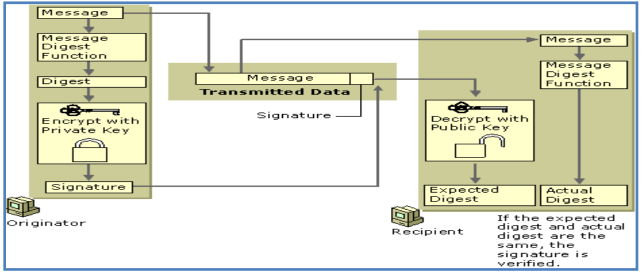

Figure 4 (Basic RSA Data **Security Digital Signature Process)**

To verify the contents of digitally signed data, the recipient generates a new message digest from the data that was received, decrypts the original message digest with the originator's public key, and compares the decrypted digest with the newly generated digest. If the two digests match, the integrity of the message is verified. The identify of the originator also is confirmed because the public key can decrypt only data that has been encrypted with the corresponding private key.

Digital Signature Security Standard

Another widely used technology for creating digital signatures is the Digital Signature Security Standard (DSS) that was developed by the National Security Agency and adopted by the United States government as its digital-signature standard. DSS defines the Digital Signature Algorithm (DSA), which functions in a manner similar to RSA. Although similar to RSA, DSA does not encrypt message digests with the private key or decrypt the message digest with the public key. Instead, DSA uses special mathematical functions to generate a digital signature composed of two 160-bit numbers that are derived from the message digest and the private key. DSA uses the public key to verify the signature, but the verification process is more complex than RSA.

The digital signature processes for DSA and RSA are generally considered to be of equal strength. However, DSA requires the use of the SHA-1 message digest function to ensure strong digital signatures. RSA can be used with other message digest functions (besides SHA-1) that might produce weaker digital signatures. Because the DSA signature verification process increases computer processor load significantly, relative to the verification process for RSA (all other conditions being equal), the RSA digital signature process generally provides better overall performance.

Because DSA is used only for digital signatures and makes no provisions for data encryption (for example, to provide secure secret key exchange), DSA is usually not subject to the export or import restrictions commonly imposed on RSA cryptography technology. Therefore, DSS digital signature technology can often be used when RSA digital signature technology cannot be used because of government-imposed export or import restrictions.

Uses for Digital Signatures

Anyone with the public key can use it to perform a validity check of digital signatures created by the private key. Only a digital signature created by the appropriate private key decrypts and validates properly with the public key. If a different private key was used to sign the data, the validity

IJERT

check fails. If the contents of digitally signed data or the digital signature have been tampered with or are corrupted, the validity check also fails. Valid digital signatures can be used to perform the following functions:

- Authenticate online entities.
- Verify the authorship or origin of digital data.
- Ensure the integrity of digital data against tampering.

Many security technologies use digital signatures. For example, Microsoft® Authenticode® can be used to digitally sign software programs, safeguarding them when they are distributed on the intranet or Internet to help counter the threat of software tampering and the spread of viruses and other malicious code. Likewise, the S/MIME protocol can be used to digitally sign e-mail messages to ensure the integrity of mail communications.

5. OTHER EMERGING APPLICATIONS

The use of cryptographic techniques is also emerging in other signal processing domains, often driven by the need to protect the privacy of user-related information. In smart electricity grids, for instance, the energy demand of individual users is monitored by smart meters for the purpose of load balancing in the energy network and real-time energy price negotiations .Unfortunately, it is easy to infer users' behavior from the observed energy demand .Signal processing solutions are emerging that bring cryptographic techniques to smart meters such that load balancing and price negotiations can be performed by the energy distributor, but in such a way that, at the same time, the privacy of the user is protected .A common service provided in social networks is to generate recommendations for finding new friends, groups and events using collaborative filtering techniques. The data required for the collaborative filtering algorithm is collected from sources such as the user's profile friendships, click logs, and other actions. The service providers often also have the right to distribute (processed) data to third parties for completely unrelated commercial or other usage. In a solution is described in which recommendations can be made without the service provider learning the privacy-sensitive information of the user .Medical data forms another type of privacy sensitive information. In the focus is on the analysis of ECG data by a remote server. The security set-up considers a situation in which the server is asked to elaborate a diagnosis by relying on the ECG profile, without learning anything about the profile and even the output of diagnosis. The solution proposed in achieves such a goal by relying on garbled circuit theory. Interestingly the implementation provided permits to process a single heart beat in 3-4 seconds of CPU time, almost approaching real time processing of ECG's. In other situations, protecting the details of the processing algorithm is also important (private function evaluation). This is the case, for instance, when the service provider's rather than the user's data must be protected. In [28], a solution is described that protects the weights of a trained neural network. The rationale for doing that is that these weights may be the result of an (expensive) training process with unique data and hence are valuable information that needs to be protected. Another example of such a situation is described in [29], where a linear decision tree is applied to encrypted data without that the exact shape of the tree is revealed.

IJERT

6.Conclusion

In the sense Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret and a power full technique that is, and can be helpful for human welfare in presence and future also .their are still a lot of emerging techniques which may helpful to boost the cryptography for human welfare. This paper will encourage the further initiatives to be taken for implementation of work in such domain

7.ACKNOWLEDGMENT-

The author thanks the director of college "ANNASAHEB COLLEGE OF ENGG.& TECHNOLOGY"for financial support and alsoDr.Shaila Subbaraman (professor at ADCET)Mrs. M.N. Chvan(asst. professor at ADCET) Mr. R. A. Jadhav(asst. professor at ADCET) For the technical assistance.

8. REFERENCES

[1].EMERGING CRYPTOGRAPHIC CHALLENGES IN IMAGE AND VIDEO PROCESSING

[2]W. Puech1, Z. Erkin2, M. Barni3, S. Rane4, And R. L. Lagendijk2

[3]0 LIRMM, UMR 5506, CNRS, University Of Montpellier II, France

[4] Information Security And Privacy Lab, Delft University Of Technology, The Netherlands

[5]Department Of Information Engineering, University Of Siena, Italy

[6] Mitsubishi Electric Research Laboratories, Cambridge, MA, USA

[7] Ear Biometrics Based On Geometrical Feature Extraction
Michał Choraś
* Institute Of Telecommunication,
University Of Technology And Agriculture, ATR Bydgoszcz, Poland

[8] Nair .M And Shamir .A (1995), "Visual Cryptography," In Proc. EUROCRYPT' 94, Berlin, Germany, Vol. 950, Pp. 1–12, Springerverlag , LNCS.

[9]. Naor .M And Pinkas .B (1997), "Visual Authentication And Identification," In Proc. CRYPTO'97, Vol. 1294, Pp. 322–336, Springer-Vela LNCS.

[10]] Azeema Sultana, Dr. M. Meenakshi, "Design And Development Of FPGA Based Adaptive Thresholder For Image Processing Applications" ,Online Access

[11]Basem Alijla And Kathrein Kwaik, "OIAHCR: Online Isolated Arabic Handwritten Character
Recognition Using Neural Network", Online Access

IJERT

9. AUTHORS PROFILE –

Name	: Mr. Abidali G. Surati
Designation	: Assistant Professor
Qualification	: B.E.(Electronics)
Experience	: 4 Yrs
Area of Specialization	: Power Electronics, Electronics Communication System

Name	: Mr. Ritesh Anant Jadhav
Designation	: Assistant Professor
Qualification	: M.E (App)
Experience	: -
Area of Specialization	: Wireless Communication

Name	: Mr. Harshad Daingade
Designation	: Assistant Professor
Qualification	: B.E.(E&Tc.)
Experience	: 1 Year
Area of Specialization	: Microprocessor , Microcontroller

Name	: Mr. Aharuddin .A.Shaikh
Designation	: B.E student
Qualification	: B.E.(E&Tc.)(App)
Experience	: none
Area of Specialization	: Microelectric mechanical system