INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 228-237

e-ISSN : 2583-1062

Impact Factor : 5.725

A NEW HYBRID VIDEO ENCRYPTION TECHNIQUE BASED ON AES CRYPTOGRAPHY

Anjali Krishna[1], Sarika Jain[2], S Geetha[3]

[1]M.Sc-CFIS, Center of Excellence in Digital Forensics, Dr. M.G.R Educational and Research Institute, Chennai 600 089, Tamilnadu, India

[2]Center of Excellence in Digital Forensics, Dr. M.G.R Educational and Research Institute, Chennai 600 089, Tamilnadu, India

[3]Head of the Department, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

ABSTRACT

The far and wide IoT and the Electronic world and the utilization of sight and sound recordings and pictures over the Web have made an expansion in the need safeguard these media information. Video encryption is generally utilized as a procedure for giving security to computerized video. In this paper, a video security method is created; utilizing the confusion framework for encoding fundamental and imperative information, and it uses a tumultuous guide as a solitary important generator, which produces significant utilized for document encryption process. Scattered frameworks have been productively utilized for sight and sound security. Turbulent cryptography has fantastic points of interest like pseudo arbitrariness, as well as aversion to starter issues. This Video encryption strategy has effectively planned and completed, the tests and assessment results have uncovered the do well of the scrambled information in regards to slipped by time and security.

Keywords: Hybrid video encryption, AES cryptography, technique.

1. INTRODUCTION

Watermarking, which is implanted with a film contains a mystery message inside the host data, is a particular sort of data hiding away with a substitute explanation than steganography. In proposed framework, the new protected film is implanted with watermark, and it is delivered in around the world. Any unapproved client records the film through camcorder and afterward transferred to the web. Presently client demands the film to the server. The server at first validates the video regardless of whether this video is inserted with watermark through the watermark extraction in the event that the film is implanted with watermark, client can't see the record or download the film, the actual server will decline the solicitation from satisfy. A watermarking calculation should guarantee that the watermark implanted in a host video doesn't fundamentally influence the visual nature of this video. A watermarking calculation is subtle in the event that the natural eye can't recognize a unique and watermarked video. In second strategy, the mystery key is created for the protected watermarking video, where the server at first request secret key then just the video is permitted to transfer. On the off chance that the client isn't having the substantial key then the client isn't permitted to post the protected video which is inserted with watermark.

2. LITERATURE SURVEY

Chun-Shien Lu et.al., we propose a novel multipurpose watermarking scheme, in which robust and fragile watermarks are simultaneously embedded, for copyright protection and content authentication. By quantizing a host image’s wavelet coefficients as masking threshold units (MTUs), two complementary watermarks are embedded using cocktail watermarking and they can be blindly extracted without access to the host image. For the purpose of image protection, the new scheme guarantees that, no matter what kind of attack is encountered, at least one watermark can survive well. On the other hand, for the purpose of image authentication, our approach can locate the part of the image that has been tampered with and tolerate some incidental processes that have been executed. Experimental results show that the performance of our multipurpose watermarking scheme is indeed superb in terms of robustness and fragility.

Chun-Shien Lu et.al., a novel image protection scheme called “cocktail watermarking” is proposed in this paper. We analyze and point out the inadequacy of the modulation techniques commonly used in ordinary spread spectrum watermarking methods and the visual model-based ones. To resolve the inadequacy, two watermarks which play complementary roles are simultaneously embedded into a host image. We also conduct a statistical analysis to derive the lower bound of the worst likelihood that the better watermark (out of the two) can be extracted. With this “high” lower bound, it is ensured that a “better” extracted watermark is always obtained. From extensive experiments, results indicate that our cocktail watermarking scheme is remarkably effective in resisting various attacks, including combined ones.

Eugene T. Lin et.al., the use of digital video offers immense opportunities for creators; however, the ability for anyone to make perfect copies and the ease by which those copies can be distributed also facilitate misuse, illegal copying and distribution (“piracy”), plagiarism, and misappropriation. Popular Internet software based on a peer-to-peer architecture has been used to share copyrighted movies, music, software, and other materials. Concerned about the consequences of illegal copying and distribution on a massive scale, content owners are interested in digital rights management (DRM) systems which can protect their rights and preserve the economic value of digital video. A DRM system protects and enforces the rights associated with the use of digital content. Unfortunately, the technical challenges for securing digital content are formidable and previous approaches have not succeeded. We overview the concepts and approaches for video DRM and describe methods for providing security, including the roles of encryption and video watermarking. Current efforts and issues are described in encryption, watermarking, and key management. Lastly, we identify challenges and directions for further investigation in video DRM.

Christophe De Vleeschouwer et.al., digital watermarking consists of hiding subliminal information into digital media content, also called host data. It can be the basis of many applications, including security and media asset management. In this paper, we focus on the imperceptibility requirement for image watermarking. We first provide a functional inventory of image watermarking applications and emphasize the dependency between the application purpose and its need for invisibility. Then, we present a global framework common to most existing watermarking systems. It illustrates the methodology followed to translate human vision research into watermarking technology. It suggests future prospects and highlights the need for dedicated inputs from the human vision community.

Fabien A. P. Petitcolas et.al., information-hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly.

Military communications systems make increasing use of traffic security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver, or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. Criminals try to use whatever traffic security properties are provided intentionally or otherwise in the available communications systems, and police forces try to restrict their use. However, many of the techniques proposed in this young and rapidly evolving field can trace their history back to antiquity, and many of them are surprisingly easy to circumvent. In this article, we try to give an overview of the field, of what we know, what works, what does not, and what are the interesting topics for research.

3. SCOPE OF PROJECT

- Subsequent to investigating a few examination papers, we accompany the rundown underneath limitations that should be thought of:
- There is a significant requirement for utilizing explicit security and furthermore decoding procedures.
- Video encryption and Decoding procedures are joined to offer substantially more security.
- Interest for limiting the assurance and decoding time, which will with certainty not impact security strength.
- There is a few wellbeing and security framework which can protect the secret key spillage.
- We can utilize dividers-based security to give significantly more impact.
- The information should be changed in particular configurations to foster the disarray cycle.

4. OBJECTIVES

Today, genuine enhancement concerns and higher layered search space are as of now modern, so they stay in basic overwhelming. In a few fields, for example, engineering, heuristic promoting strategies have been utilized. Man-made reasoning, organization strategies, mechanics, business financial matters, booking, transportation, integrated choice making, and furthermore arrangements gauge Showcasing relates to finding an OK ideal answer for a specific issue one of a great deal of plausible ones. Showcasing movement is generally different into a hunting issue in a multi-layered region. Basically, the hunt plans to moderate or expand a goal highlight that surveys a candidate's quality for an answer that is generally characterized by an inquiry locale point. Meta-heuristics are cherished by near enhancement moves toward that offer practical options in a sensible period.

5. EXISTING SYSTEM

The visual mixture video encryption on a computerized record is somewhat straightforward: you can make a picture that has your copyright image or other distinguishing visual on the actual image. On the off chance that individuals duplicate the image, you can in any case yours. You can decide to place an immense imprint in the center, or you can put a more unobtrusive blemish as an afterthought. While it more straightforward to see the whole picture while utilizing a little imprint, the weakness is that it tends to be effectively eliminated by a deceitful individual utilizing a basic picture manager.

While this is almost unimaginable with a bigger imprint in the picture, areas of strength for the is that it harder to see the actual picture. In certain applications, a mediocre right hand or a channel director desires to add some extra message, like the beginning data, picture documentation or validation information, inside the scrambled picture however he doesn't have a clue about the first picture content. A few boundaries are installed into few scrambled pixels, and the of the other encoded pixels are compacted to make a space for obliging the extra information and the first information at the positions involved by the boundaries

6. PROPOSED SYSTEM

Since media data contains some overt repetitiveness, e.g., recordings, they are normally packed to save the complete stockpiling or transmission cost. To keep submissive with correspondence frameworks, the encryption procedure, taking into account the pressure, scramble a few delicate boundaries all through the pressure. Subsequently, we utilize turbulent planning to raise the video encryption framework's security, and we de-mix the evacuation makes the client avoid the hole of the forefront things' shapes. To start with, the client records security video cuts, which are then gotten by our proposed cluttered planning-based encryption procedure. The scrambled checking video cuts are moved to the cloud server, where the forefront extraction equation is working on the encoded recordings. The outcomes are moved back to the client, in which the expulsion results are decoded to acquire the extraction prompts express video records. The expulsion accuracy in the security video cuts is like that in the normal video cuts.

6.1 Modules

- Slicing
- Motion compensation
- Motion vector prediction
- Block transformation and encoding
- Macro block ordering

6.2 Modules Descriptions Slicing

In general, a coded picture is divided into one or more slices. Slices are self- contained and can be decoded and displayed independently of oth er slices. Hence, intraprediction of DCT coefficients and coding parameters of a macro block is restricted to previous macro blocks within the same slice. This feature is important to suppress error propagation within a picture due to the nature of variable length coding. In regularencoding, when FMO is not used, slices contain a sequence of macro blocks in raster scan order. However, FMO allows the encoder to create what is known as slice groups.Each slice group contains one or more slices and macro blocks can be assigned in anyorder to these slices. The assignment of macro blocks to different groups is signaled bya syntax structure called the “slice group id”.

Slice Types

H.264 defines five different slice types: I, P, B, SI and SP.

I slices or “Intra” slices describe a full still image, containing only references to itself. Avideo stream may consist only of I slices, but this is typically not used. However, the first frame of a sequence always needs to be built out of I slices.

P slices or “Predicted” slices use one or more recently decoded slices as a reference (or “prediction”)

for picture construction. The prediction is usually not exactly the same as the actual picture content, so a “residual” may be added.

B slices or “Bi-Directional Predicted” slices work like P slices with the exception that former and future I or P slices (in playback order) may be used as reference pictures. For this to work, B slices must be decoded after the following I or P slice.

Motion Compensation

Since MPEG-1, movement pay is a standard coding device for video pressure. Utilizing movement remuneration, movement between edges can be encoded in an extremely proficient way. A common P-type block duplicates a region of the last decodedoutline into the ongoing casing support to act as an expectation. On the off chance thatthis block is doled out a nonzero movement vector, the source region for this duplicate cycle won't be equivalent to the objective region. It will be moved by certain pixels, permitting to accommodate for the movement of the article that involves that block. Movement vectors need not be number qualities: In H.264, movement vector accuracyis one-quarter pixel (one eighth pixel in chroma). Addition is utilized to decide the powervalues at non-number pixel positions. Moreover, movement vectors might highlight districts beyond the picture. For this situation, edge pixels are rehashed.

Motion Vector Prediction

Since nearby blocks will quite often move in similar bearings, the movement vectors are likewise encoded utilizing expectation. At the point when a block's movement vector is encoded, the encompassing blocks' movement vectors are utilized to gauge the ongoingmovement vector. Then, at that point, just the contrast between this expectation and thereal vector is put away.

Block Transformation and Encoding

The essential picture encoding calculation of H.264 utilizes a detachable change. The method of activity is like that of JPEG and MPEG, yet the change utilized is definitely not a 8x8 DCT, yet a 4x4 whole number change got from the DCT. This change is exceptionally straightforward and quick; it tends to be processed utilizing just augmentations/deductions and twofold moves. It decays the picture into its spacial recurrence parts like the DCT, yet because of its more modest size, it isn't as inclined tohigh recurrence "mosquito" relics as its ancestors A picture block B is changed to B0 utilizing the accompanying recipe. The vital post-scaling step is incorporated intoquantization (see beneath) and consequently excluded:

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & -1 & -2 \\ 1 & -1 & -1 & 1 \\ 1 & -2 & 2 & -1 \end{pmatrix}$$

$$B' = MBM^T$$

The fundamental usefulness of the H.264 picture change process is as per the following: For each block, the genuine picture information is deducted from the expectation. The subsequent lingering is changed. The coefficients of this change are isolated by a consistent number. This technique is called quantization; it is the main move toward theentire encoding process that is really lossy. The divisor utilized is known as thequantization boundary; different quantization boundaries are utilized for luma andchroma channels. The quantized coefficients are then perused out from the 4x4 coefficient grid into a solitary 16-component examine. This output is then encoded utilizing modern (lossless) entropy coding. In the decoder, these means are acted in turned around request.

Macroblock Ordering

In this paper, we utilize the express task of macroblocks to cut gatherings to conceal messages in the video transfer. Since macroblocks can be inconsistent allocated to cut gatherings, we propose to utilize the cut gathering ID of individual macroblocks as a signof message bits. Expect for example that two cut bunches are utilized, the distribution of a macroblock to cut bunch 0 shows a message piece of 0 and the designation of macroblock to cut bunch 1 demonstrates a message piece of 1. Thus, one message bitfor every macroblock can be conveyed.

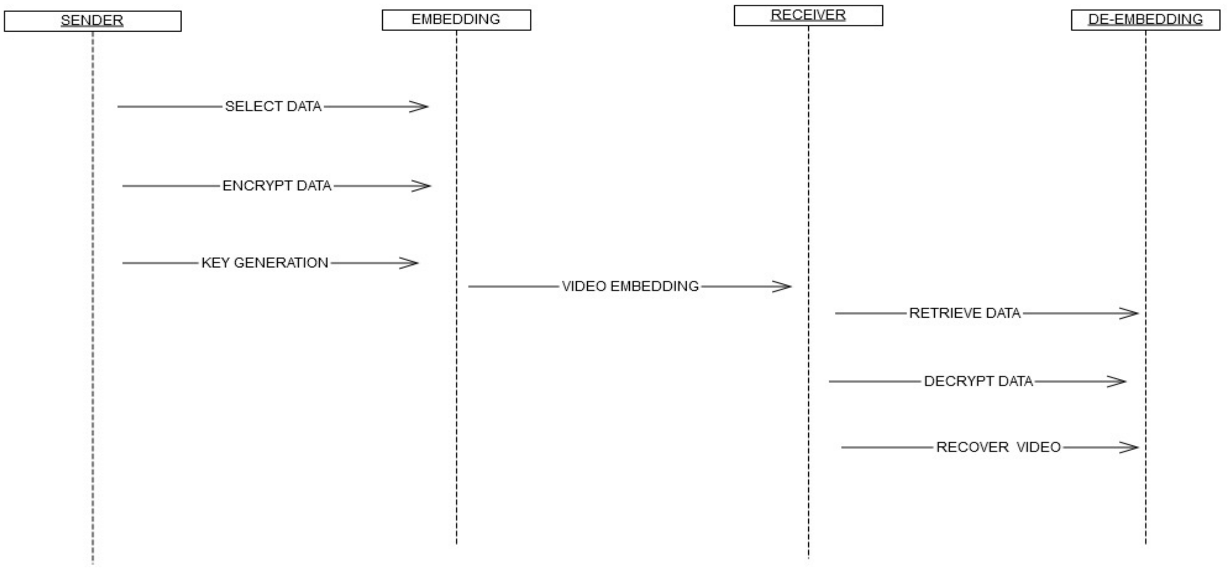


Figure 1. Sequence Diagram

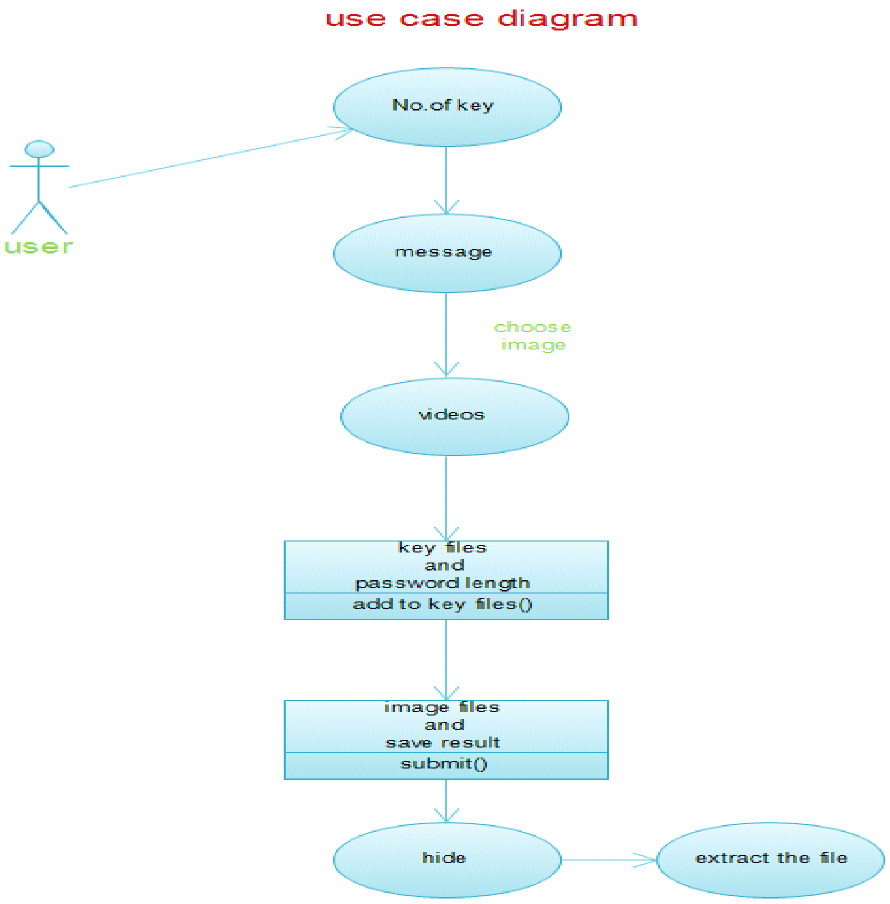


Figure 2. Use Case Diagram

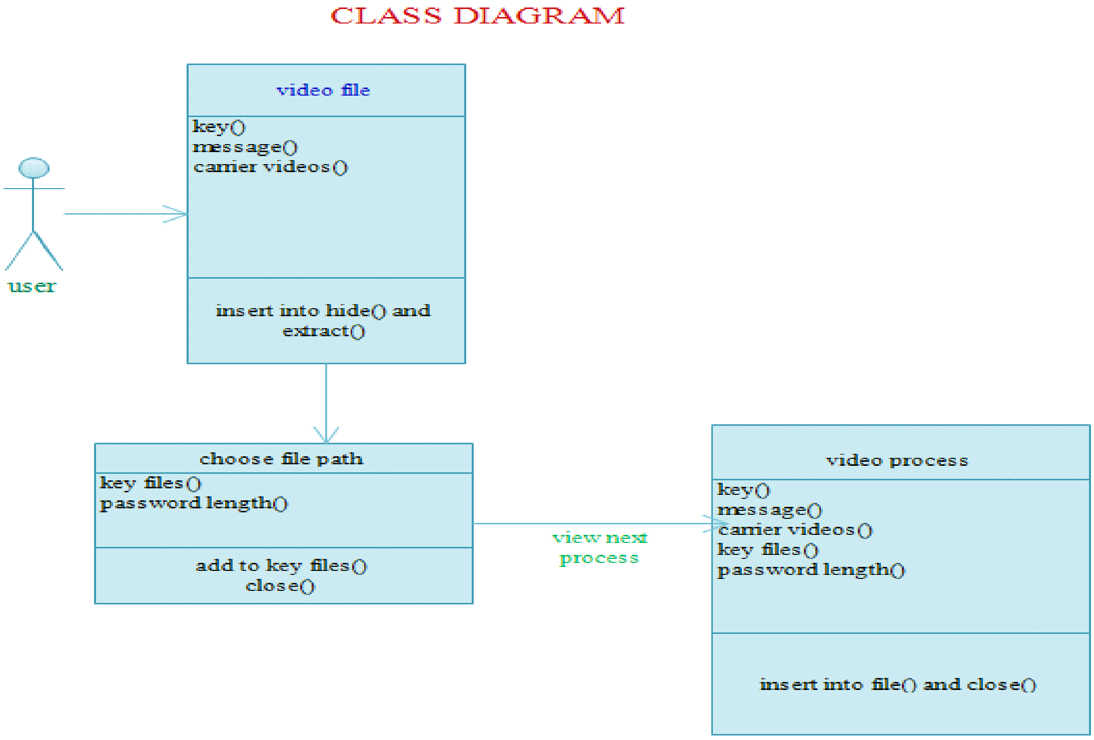


Figure 3. Class Diagram

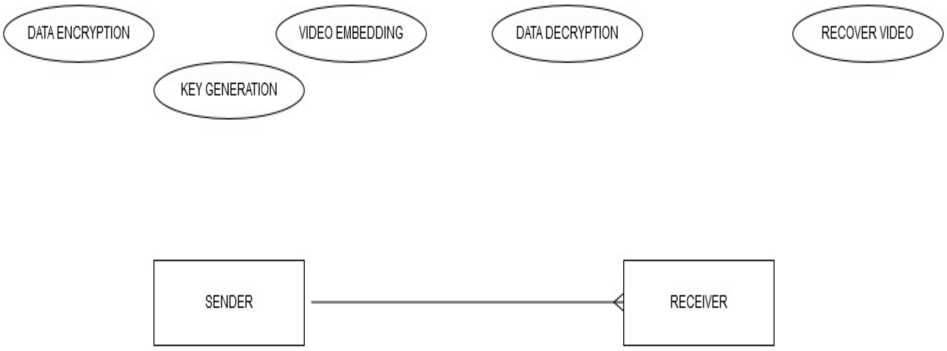
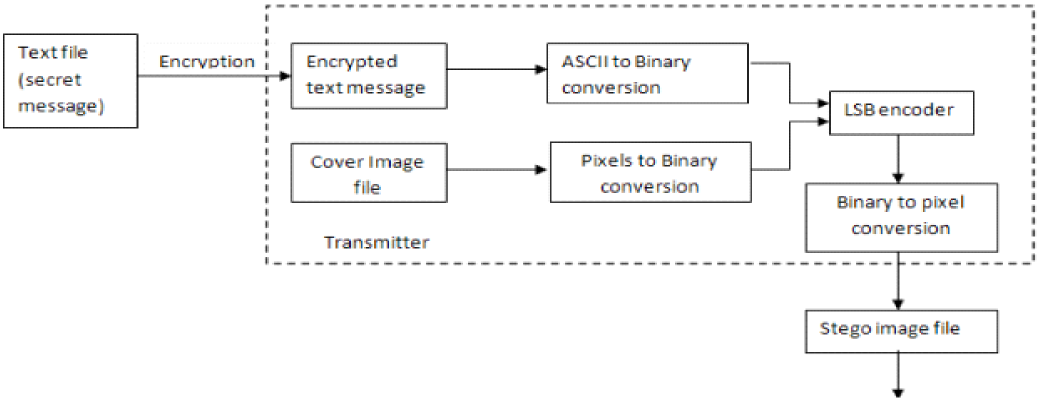


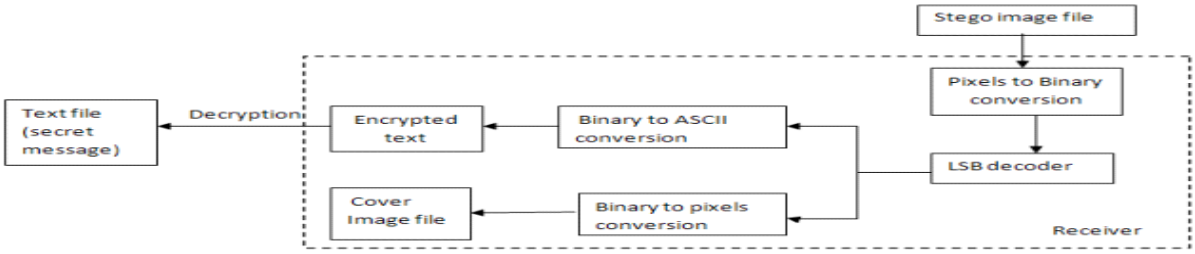
Figure 4. ER-Diagram

DFD

Level-0


Text file (secret message)
Encryption
Encrypted text message
ASCII to Binary conversion
Cover Image file
Pixels to Binary conversion
LSB encoder
Binary to pixel conversion
Transmitter
Stego image file

Level-1


Stego image file
Pixels to Binary conversion
LSB decoder
Binary to ASCII conversion
Encrypted text
Decryption
Text file (secret message)
Binary to pixels conversion
Cover Image file
Receiver

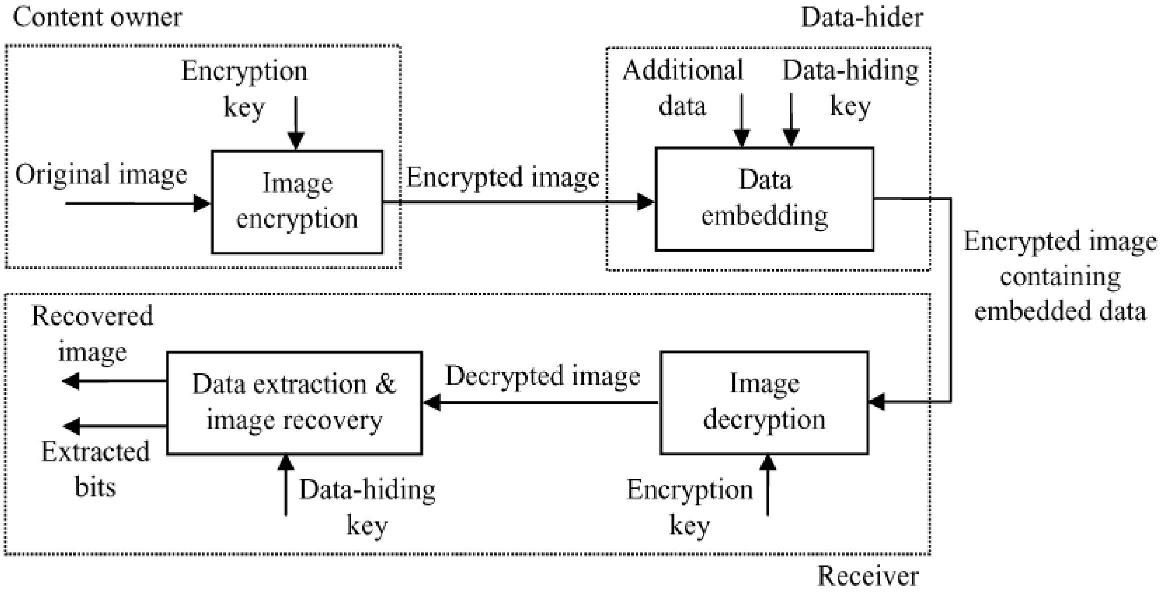
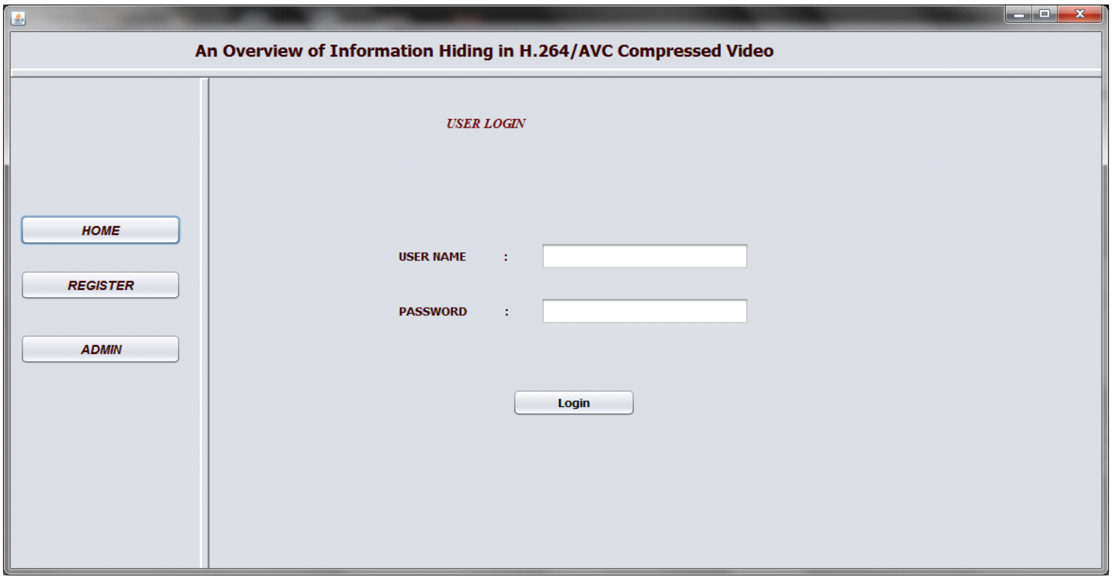


Figure 5. Overall Flow Diagram

Screenshot

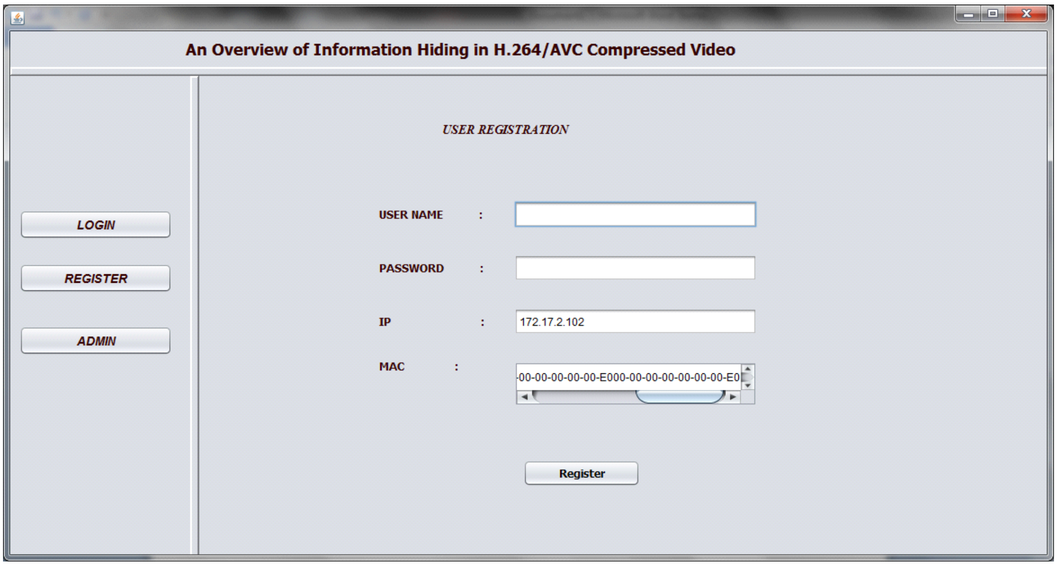


An Overview of Information Hiding in H.264/AVC Compressed Video

USER LOGIN

USER NAME :

PASSWORD :

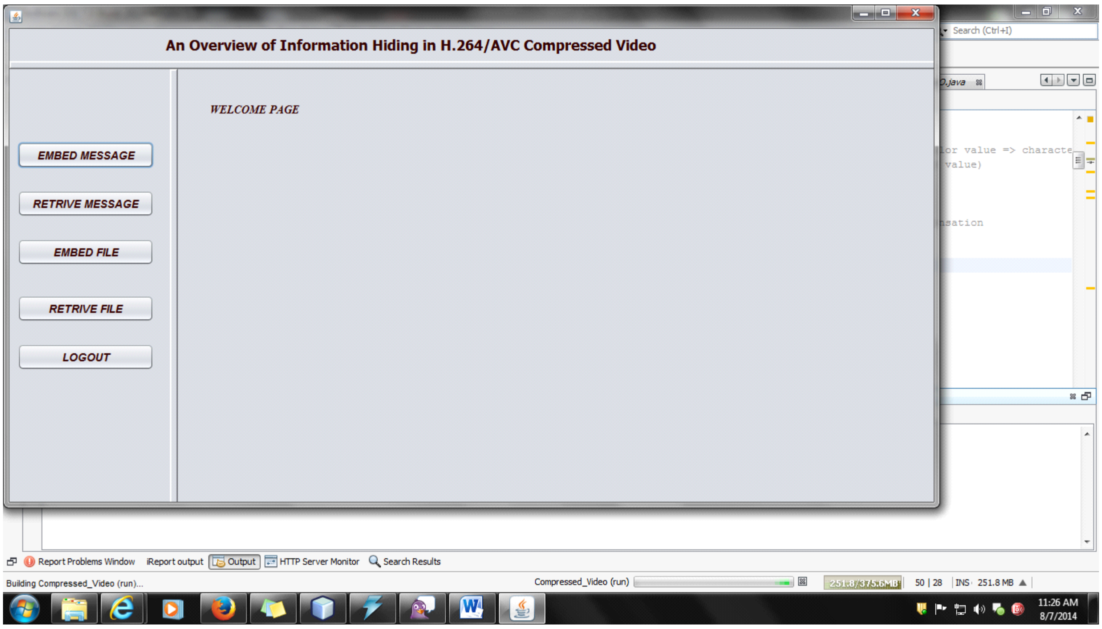

An Overview of Information Hiding in H.264/AVC Compressed Video
USER REGISTRATION
LOGIN
REGISTER
ADMIN
Register

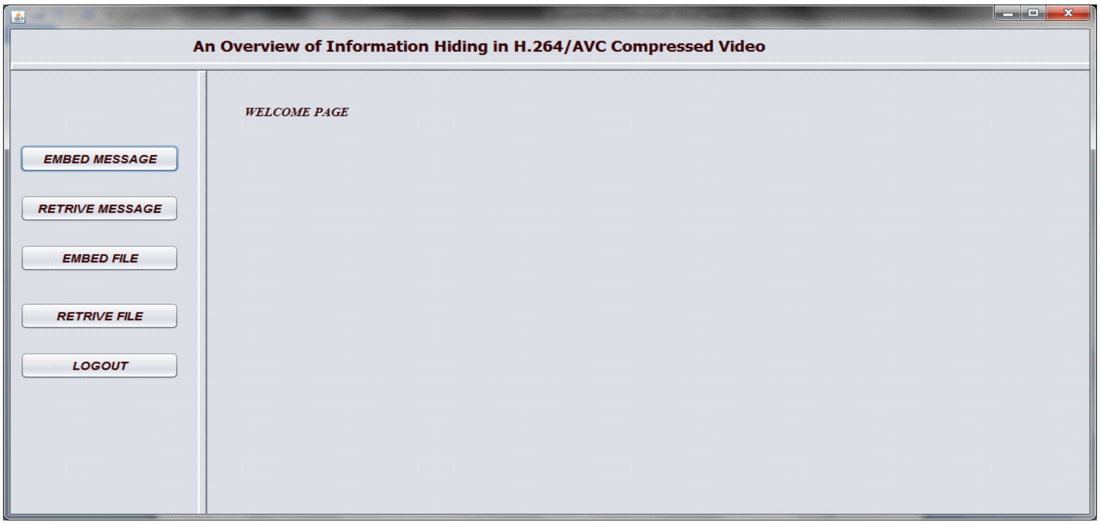
USER NAME :

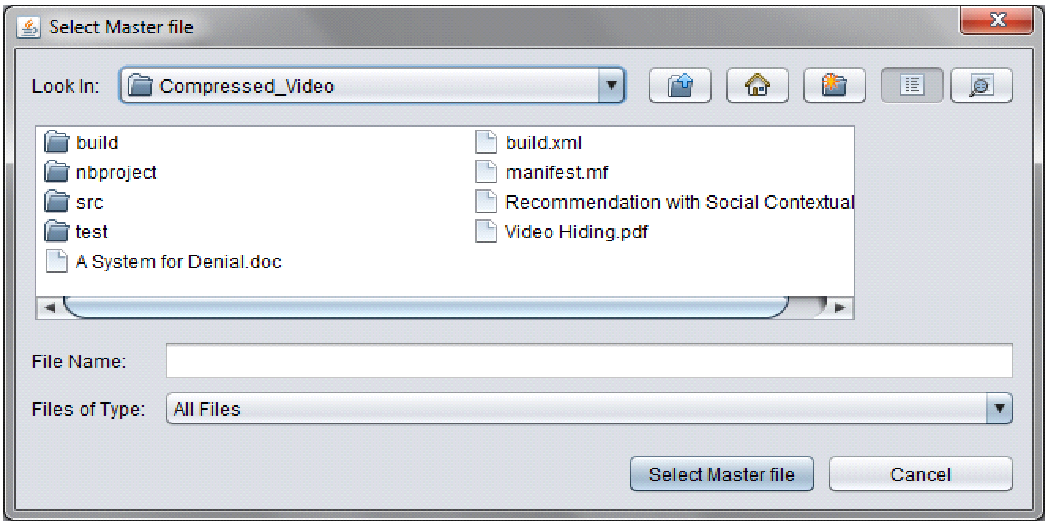
PASSWORD :

IP : 172.17.2.102

MAC : -00-00-00-00-00-E000-00-00-00-00-00-00-E0

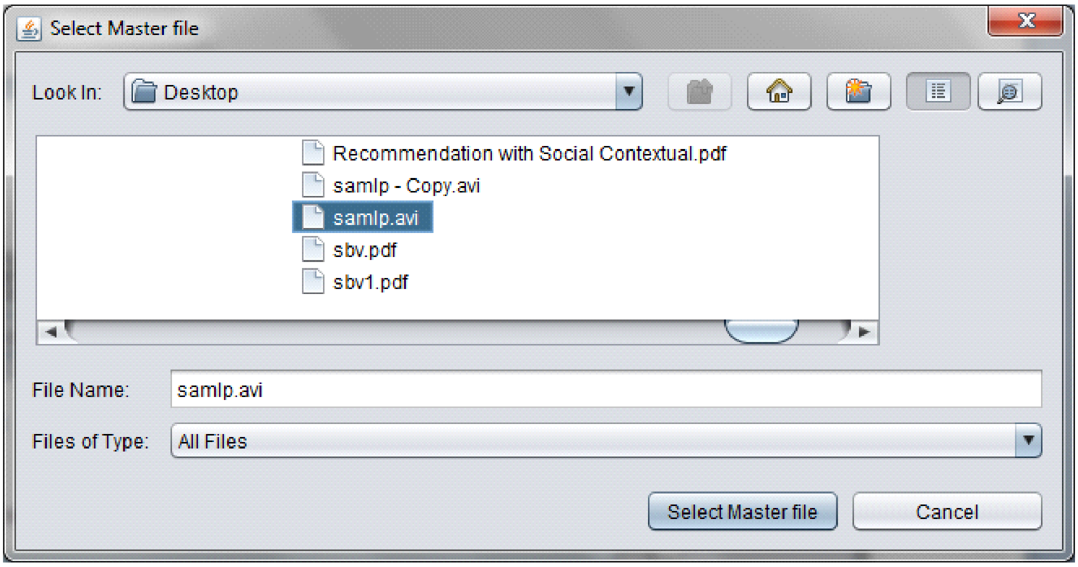





Look In: Compressed_Video

File Name:

Files of Type: All Files


Look In: Desktop

File Name: samlp.avi

Files of Type: All Files

7. CONCLUSIONS AND FUTURE WORK

In the present paper, a reliable diffusion plan is suggested to address the effectiveness and protection imperfections of the traditional permutation-diffusion kind of picture cryptosystems. This scheme makes full use of the level of sensitivity residential property of the hybrid video encryption systems, and a minor difference in the image can be transferred to the hybrid video iteration and afterward produces different vital stream elements. The cryptosystem's dispersing effect can be considerably accelerated in the supplementary diffusion treatment through this system, and the cryptosystem can resist chosen/known-plaintext assaults successfully. Experimental results have proved the higher performance and the safety and security level of the recommended scheme. These renovations can encourage the useful applications of permutation-diffusion style hybrid-based image cryptosystems. In this paper, a file encryption plan for images or videos exists based on the spatiotemporal disorder system. A stream cipher is built based upon the pseudorandom sequences produced by the spatiotemporal lattices. After that, the series is made use of to encrypt the chosen specifications in each image block. The plan's performances are evaluated and assessed, including the security of the stream cipher, the affective safety of the encrypted videos, and the result on compression performance (compression proportion and computational price). The results reveal that the proposed stream cipher pleases the demand for safe and secure encryption principles. The encrypted photos or video clips are safe in perception. The encryption procedure does not transform the compression proportion, and the scheme enhances little computational expense compared with video file encryption. These make it an ideal option for video security applications.

REFERENCE

[1] E. Smith and L. A. E. Schuker, “Studios unlock DVD release dates,” The Wall Street Journal, Feb. 2010.

[2] J. D. Koch, M. D. Smith, and R. Telang, “Camcording and film piracy in asia-pacific economic cooperation economies,” International Intellectual Property Institute, Aug. 2011.

[3] B. Stelter and B. Stone, “Digital pirates winning battle with studios,” The New York Times, Feb. 2009.

[4] “Economic consequences of movie piracy – Australia,” Jan. 2011.
[5] A. Piva, F. Bartolini, and M. Barni, “Managing copyright in open networks,” IEEE Internet Computing, vol. 6, no. 3, pp. 18–26, May 2002.
[6] C. S. Lu and H. Y. M. Liao, “Multipurpose watermarking for image authentication and protection,” IEEE Transactions on Image Processing, vol. 10, no. 10, pp. 1579–1592, Oct. 2001.
[7] C. S. Lu, S. K. Huang, C. J. Sze, and H. Y. M. Liao, “Cocktail watermarking for digital image protection,” IEEE Transactions on Multimedia, vol. 2, no. 4, pp. 209–224, Dec. 2000.
[8] “Steganography,”[Online].Available: http://en.wikipedia.org/wiki/Steganography, 23 Dec. 2003.
[9] N. Terzija, Robust digital image watermarking algorithms for copyright protection, Ph.D. thesis, University Duisburg-Esen, Oct. 2006.
[10] C. I Podilchuk and E. J. Delp, “Digital watermarking: algorithms and applications,” IEEE Signal Processing Magazine, vol. 18, no. 4, pp. 33–46, Jul. 2001.