Volume 4, No. 4, April 2013
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

EFFICIENT IDENTIFICATION OF HIDDEN VIDEOFILES EXPLOITATION COMPRESSION AND SECRET RECOGNITION TECHNIQUES

Santhosh Kumar S*, Kishore A and Mr. Chandrasekaran
Bharath University, Chennai, India
jeeva45@gmail.com

Abstract- To view the hidden video files by exploitation secret recognition system. [1] Video files are incorporated exploitation compression and extracted by decompression techniques. Cheating the hackers by showing solely the duplicate video file. [2] Making a brand new video player to play the incorporated files. Viewing the initial video file is feasible once trigger is generated. Files are incorporated exploitation compression algorithms. Here the MSA (Meheboob, Saima and Asoke) formula is employed to cyphering the key message and introduced a brand new organization methodology for generating the irregular key matrix that contains all 256 characters in sixteen X sixteen matrix to encrypt plain computer file and to decipher cipher computer file. To make the compression and therefore the decompression method all secured the authors has introduced multiple compression and multiple decompression strategies. [3] The utmost length of the text key is often of sixteen characters long and it's going to contain any character (ASCII code zero to 255). From the given text key one will calculate the organization variety and therefore the encoding variety exploitation a formula. Furthermore the multiple compression methodology makes the system more secured. To cover encrypted secret video enter the duvet file the authors have inserted within the 4-th little bit of every character of encrypted message enter eight consecutive bytes of the duvet file. The authors have introduced secret for concealment information within the cowl file. This methodology is also the foremost secured methodology in defense for causation some confidential video file.

INTRODUCTION

The goal of the project is to secure the key video files and think about that secret video files with efficiency by mistreatment compression and parole recognition techniques. With the fast enlargement of the net and transmission technology, video concealment based on compression technique and cheating the hackers by showing the duplicate video file is secured methodology. Videos are incorporate mistreatment compression algorithms. The compressed file having the new extension (own extension). Viewing the initial video file is feasible once trigger is generated. Here the MSA (Meheboob, Saima and Asoke) algorithmic rule is employed to encrypting the key video file.

We introduced a brand new organization method for generating the irregular key matrix that contains all 256 characters in sixteen X sixteen matrixes to inscribe plaintext file and to decipher cipher computer file. To create the compression and also the decompression method completely secured, we introduced multiple compression and multiple decompression strategies. MSA methodology is completely keen about the random text key that is to be equipped by the user. [4]

The maximum length of the text key are often of sixteen characters long and it's going to contain any character (ASCII code zero to 255). From the given text-key one will calculate the organization variety and also the cryptography variety mistreatment AN algorithmic rule. [5] what is more the multiple cryptography methodology makes the system any secured. To {cover} encrypted secret message within the cover file the authors have inserted within the 4-th little bit of every character of encrypted message come in eight consecutive bytes of the duvet file. We introduced parole protection security methodology with multiple compression and decompression for concealment original video file within the duplicate video file. This methodology is also the foremost secured methodology in defense for causation some confidential video file.[6]

The Video files are transmitted into the frames. [7] Frames are reborn into pattern image files. Then the pattern pictures are transmitted over to the text files. Then the cryptography key distribution with the code. [8] Code are generated with the assistance of MSA algorithmic rule. [9]

LITERATURE REVIEW

Shuichi Takano, Kiyoshi Tanaka and Tatsuo Sugimura (2010) projected a replacement information concealment theme via stenographic image transformation. That is completely different from standard information concealment techniques. The transformation is achieved within the frequency domain and therefore the conception of Fourier filtering technique is employed. Associate Input Image is reworked into a form image, which may be utilized in laptop Graphic (CG) applications. Unauthorized users won't notice the key original image behind the form image, however notwithstanding they Apprehend that there's a hidden image it'll be tough for them to estimate the first image from the reworked image. Solely licensed users apprehend the correct keys will regenerate the first image.

The projected technique is applicable not solely as a security tool for transmission contents on web content however additionally a stenographic secret communication technique through form pictures. G Sahoo, R K Tiwari (2008) [2] projected a system for Steganography. The most goal of steganography is to speak message firmly in an exceedingly complete undetectable manner. It's been emerged as a ability of concealing non-public data within a carrier that may be thought of for all intents and concepts. Digital technology offers United States of America a replacement thanks to relate stenographic techniques as well as concealment data in digital pictures. It not solely goes well on the far side just by embedding a text in a picture, however additionally pertains to alternative media, as well as voice, text, binary files and communication channels. The matter of unauthorized repetition currently - a - days is of nice concern particularly to the music, film, book and code business industries. To beat such sort of issues, some invisible data are often embedded in an exceedingly digital media in such the way that it couldn't simply be extracted with none specialized technique. In alternative aspect Cryptography is one in every of the effective answer to guard the info from the unauthorized users. It are often mentioned here that though by the employment of cryptologic techniques we will convert the info into a cipher text, that is in undecipherable format, we have a tendency to cannot hide the existence of constant information.

Thus Cryptography in alone isn't sufficient to guard the info against the unauthorized access by unauthorized users.

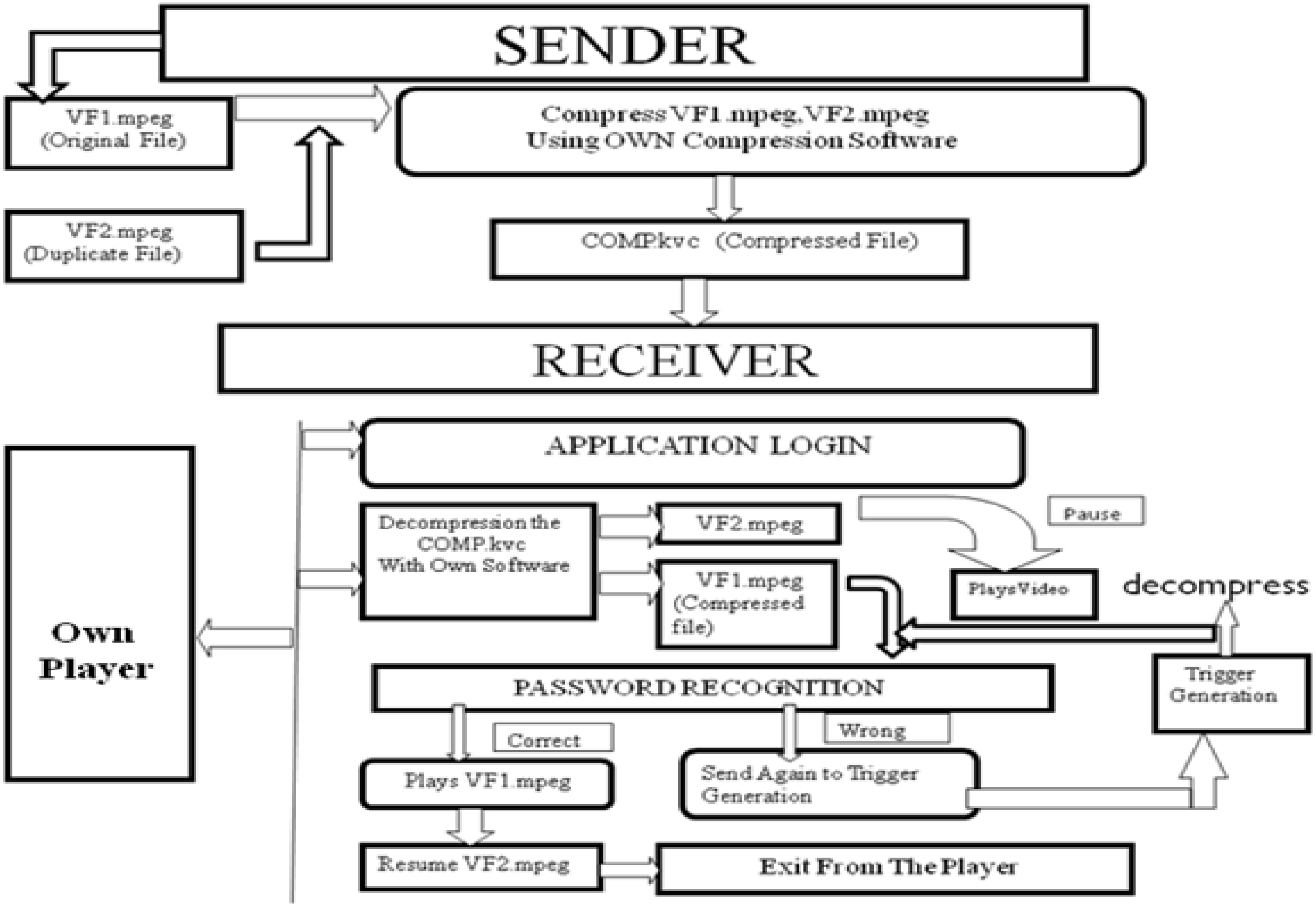
EXISTING SYSTEM

The existing Stenographic system for image transformation is merely for the image and text activity method. This method isn’t supported for video files. An input image is remodeled into a form image which might be utilized in pc graphic applications. The quantity knowledge of knowledge of information to be hidden isn't up to the host signal whereas it's generally restricted within the standard data activity scheme

PROPOSED SYSTEM

Using stenographic technique for video transformation. This method is absolutely supported for video files. Quite one video files is integrated using our own Compression software package. Compressed video files square measure having the new extensions. This extension is our own extension (.kvc). The compressed file with our own extension is Plays solely in our own video player (media player). In our system we have a tendency to conjointly develop a brand new media player. Protection of the video files is fully challenged for the hackers.

ARCHITECTURE DIAGRAM


SENDER
VF1.mpeg (Original File)
VF2.mpeg (Duplicate File)
Compress VF1.mpeg,VF2.mpeg Using OWN Compression Software
COMP.kvc (Compressed File)
RECEIVER
APPLICATION LOGIN
Own Player
Decompression the COMP.kvc With Own Software
VF2.mpeg
VF1.mpeg (Compressed file)
Pause
Plays Video
decompress
Trigger Generation
PASSWORD RECOGNITION
Correct
Wrong
Plays VF1.mpeg
Send Again to Trigger Generation
Resume VF2.mpeg
Exit From The Player

LIST OF MODULE

a. Compression Implementing for Video Files
b. Implementation of Protection to the video files
c. Implementation of video player

MODULE DESCRIPTION

Compression Implementing for Video Files:

This module involves the Implementation of Compression Software. More than one video files are compressed here.

Original video file is compressed and it again compressed with duplicate video file and forms as a single compressed file. Video files compression are done by our own compression software. After compression, compressed file having the new extension (own extension).This video files Compression method is more efficient than other methods. Multiple Compression and Decompression are done here.

Implementation of Protection to the Video files:

Compressed file having each original (compressed) and duplicate video files. Original file is hidden here and it absolutely was Arcanum protected. To view any of these files decompression is required. Multiple compression and decompression has done by mistreatment MSA algorithmic rule. Decompressions are often worn out our own code solely. Admin person solely allowed to press the video files. Because the same method Admin solely able to see the first video files when getting into the right Arcanum in our own media player. Unauthorized users won't notice the key original video file behind the duplicate video file, however albeit they apprehend that there's a hidden secret video it'll be troublesome for them to estimate the initial video file from the remodeled duplicate video file. Solely licensed users United Nation agency apprehends the right keys will regenerate the initial video file. The planned methodology is applicable not solely as a security tool for transmission contents on sites however additionally a stenographic secret communication methodology through form pictures.

Implementation of Video Player:

In this module our own media player developing method is represented. By gap the compressed come in our created Media Player decompression is completed mechanically. It will play solely the duplicate video file. The original video files are going to be vie once the second decompression has done. This second decompression has done once generating the trigger and enters the right trigger price. If the trigger price isn't correct, then the viewing of original video file isn't doable. By default, player solely plays the duplicate video file unceasingly till the right trigger priceis given by the user.

Unauthorized users area unit ready to see the video solely in windows media player (for purpose of cheating the hackers). Solely the approved or admin user’s area unit ready to play or see the video files in our own created media player.

CONCLUSION

In the gift work we have a tendency to attempt to infix some secret video come inside any cowl video file in compressed kind, so nobody are able to extract the first video file. Here we alter 4-th bit from LSB little bit of the quilt file. Our coding methodology will use most coding number=64 and most organization number=128. The key matrix is also generated in 256! Ways in which. Thus in essence it'll be terribly troublesome task for anyone to decompress the encrypted video file while not knowing the precise key matrix. Our methodology is basically stream cipher methodology and it should take vast quantity of your time if the files size is giant and also the coding range is additionally giant. These methodology advantages the entire compression and decompression method can amendment. The steganography methodology is also additional secured if we have a tendency to compress the key video file initial so write it so finally infix within the quilt file (duplicate video file). We’ve got conjointly developed associate own media player. so the files will solely play during this media player that having the actual fixed list of extensions.

REFERENCE

[1]. T.Morkel, J.H.P. Eloff and M.S.Oliver, “An Overview of Image Steganography”

[2]. Moerland, T, (2010)Leiden Institute of Advanced Computing Science, “Steganography and Seganalysis

[3]. A.Nath, S.Ghosh,M.A.Mallik, (2010) “Symmetric key cryptography using random key generator”, Proceedings of International conference on SAM-2010 held at LasVegas(USA) 12-15 July,2010, Vol-2,P-239-244.

[4].] Shawn D. Dickman,(2011) “An Overview of Steganography”.

[5]. Joyshree Nath and Asoke Nath, (2011) “Advanced Steganography Algorithm using encrypted secret message”: International Journal of Advanced Computer Science and Applications, Vol-2, No-3, Page-19-24, March (2011).

[6]. J.M.Rodrigues Et. Al., (2011)“SSB-4 System of Steganography using bit 4”.

ONLINE REFERENCE

[1]. http://msdn.microsoft.com/en-us/library/windows/desktop/dd375454(v=vs.85).aspx

[2]. http://en.wikipedia.org/wiki/Compression

[3]. http://msdn.microsoft.com/en-us/library/windows/desktop/dd375464(v=vs.85).aspx

[4]. http://www.robertyu.com/wikiperdido/Building%20a%20Steganography%20Code%20Sample%20in%20Visual%20Studio%20.NET