International Journal of Electronics Engineering (ISSN: 0973-7383)
Volume 11 • Issue 1 pp. 997-1002 Jan 2019-June 2019 www.csjournals.com

Cloud-Based Video Content Sharing Using Visual Cryptography

[1]Kumar Gaurav, [2]Dr. Sanjeev Kumar Gupta
[1]Ph.D Scholar, [2]Professor
Rabindranath Tagore University, Raisen (M.P), Bhopal, INDIA

Abstract – Video is essential element today. Today is fight for market share between licensed and illegal platforms, video content piracy has become a fully-fledged business. As an industry, video distribution has faced no greater threat than content piracy. Illicit activity conducted by professional digital pirates who operate smart interfaces, and who are capable of hacking into the most complex security systems, have threatened organizations large or small for decades. Video content security is initial demand of digital world. In this paper proposed Video frame sharing by using visual cryptography (VC). In this twofold model of the N dispenses, despite the fact that, contain no visual result and frustrate the targets of visual cryptography. The ideal security state of VC plot needs the strict interest where any t-1 or less transparency can't extricate much information in regards to the key. The mystery picture is in the meantime installed into shading halftone shares. Visual cryptography (VC) could be a mystery sharing strategy for rot a mystery picture into n transparencies, and thus the heap of any t out of n transparencies uncover the key substance. A HVC create method is anticipated that can make a possibility for mystery halftone picture into shading half-tone shares. In this paper proposed video encryption by divided different frame encrypt and arrange it same sequence.

Keywords: Cloud based Video sharing, Visual cryptography, Halftone, Video security, Video Sharing.

I. Introduction

In a media environment where video content, varying from TV shows, films and live sports, is everywhere, professional pirates prosper. Beginning with the early popularity of BitTorrent sites, illegal peer-to-peer file sharing has been encouraged as new attack surfaces have grown in their numbers. As video content can now reach a range of platforms, from creation to distribution, content leaves its digital footprint across multiple systems. On numerous channels, screens and platforms, content is managed and worked on by several teams and studios, and then distributed to audiences both locally and internationally. Every step of the production cycle is now digitalized, making content at a higher risk of piracy. And considering the interest and competition in content creation, costs are commonly directed to benefit these processes and big-name individuals and studios involved, instead of on measures to protect this content and steer pirates away.

Couple the above with our IoT obsession and we are finding ourselves caught in a large scale connected device ecosystem where content is seeing no limits. Looking at billions of devices vulnerable to illicit hacking, content distributors are asking if it is possible to gain greater control without limiting the technical growth and innovation behind these platforms. When advances in technology are vital to both fighting piracy and developing innovative content platforms, it has become a question of priority for media organizations. In a fast-paced, constantly-evolving media landscape, it's essential for media organizations to find a balance between 'content everywhere' and content protection. While targeting more audiences across many devices and platforms has been an industry breakthrough – and in some cases, a priority – it's posed new challenges for content distributors relating to content security. Visual cryptography (VC) may possibly be a division of secret sharing information. In the VC idea, a secret image is encoded into transparencies, and furthermore the content of each transparency is noise-like in order to the secret information cannot be retrieved from anyone transparency via human visual observation or signal analysis techniques. In general, a -threshold VC scheme has the subsequent properties: The stacking of any out of these VC generated transparencies will reveal the secret by perception, however the stacking of any or fewer variety of transparencies cannot retrieve any data other than the dimensions of the secret image. Naor and Shamir [3] planned a –threshold VC scheme based on basis matrices, and also the model had been more studied and extended. The connected works include the VC schemes based on probabilistic models, general access structures, VC over halftone pictures, VC for color pictures, cheating in VC, the concluding formula of VC schemes, and region incrementing VC. Contrast is one altogether the necessary performance metrics for VC schemes. Generally, the stacking revelation of the key with

higher contrast represents the higher visual quality, and thus the stacking secret with high contrast is that the goal of pursuit in VC designs .Naor and Shamir [3] define a contrast formula that has been wide utilized in several studies based on the definition of contrast, there are studies attempting to achieve the contrast certain of VC scheme. For example, Blundo et al. [7] provide the optimal contrast of VC schemes. Hofmeister et al. Encrypting a picture by random grids (RGs) was initial introduced by Kafri and Keren [2] in 1987. A binary secret image is encoded into 2 noise-like transparencies with a similar size of the original secret image, and stacking of the 2 transparencies reveals the content of the secret. Comparison RGs with basis matrices, one among the main benefits is that the dimensions of generated transparencies are unexpanded. Bharot, Gupta[4][9][10] presented a technique that will easily detect and mitigate the DDos attack and it is very easy to implement with minimum cost and overhead. Chourasia, Gupta et al.[12] defines work an effort is made to study and analyses the performance of frequently used edge detection techniques for image segmentation and also the comparison of these techniques. This work recommended multilevel thresholding for histogram-based image segmentation using OTSU algorithm. Gahalod, Gupta[6][17][21] defines, Digital image watermarking is a process in which ownership data can be hided in multimedia data, this ownership data can be extracted later on to prove the authentication of owner

1.1 Visual Cryptography Schemes

Visual cryptography could be a cryptographic technique that permits visual data (video, pictures, text, etc.) to been encrypted in such a way that the decoding is performed by the human visual system, while not the help of computers. Visual cryptography was pioneered by Moni Naorand Adi Shamir in 1994. They demonstrated a visible secret sharing scheme, wherever a picture was broken up into n shares so only someone with all n shares may decode the image, whereas any n-1 shares revealed no data concerning the original image. Every share was printed on a separate transparency, and decoding was performed by overlaying the shares. Once all n shares were overlaid, the original image would appear. Using a similar plan, transparencies is used to implemental one-time pad coding, wherever one transparency could be a shared random pad, and another transparency acts because the cipher text cryptography and steganography are well known and wide used techniques that manipulate data (messages) so as to cipher or hide their existence.

1.2 Halftone Visual Cryptography:

The main plan of half toning is to utilize the density of written dots to simulate the grey scale of pixels. For human eyes, the denser the spots are, the darker the picture is; in actuality, the sparser the specks are, the lighter the picture is. As an example, if the black dot densities of 2 areas with same size are ninetieth and 500th severally, the human visual system will perceive the difference between them: the former is darker than the latter and also the latter lighter than the previous. Therefore, we are able to} learn that the black dot density can simulate the grey-scale value of an area. Simply by dominating the black dot density of an area, half toning transforms a continuous-tone image into a binary one.
The meaningful shares generated in extended visual cryptography planned by Mizuho NAKAJIMA and Yasushi YAMAGUCHI was of poor quality that once more will increase the suspicion of information encoding. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo planned halftone visual cryptography that increases the quality of the meaningful shares. In halftone visual cryptography a secret binary pixel „P‟ is encoded into an array of Q1 x Q2 („m‟ in basic model) sub pixels, stated as halftone cell, in every of the „n‟ shares. By using halftone cells with an appropriate size, visually pleasing halftone shares is obtained. Additionally maintains contrast and security.

1.3 Cloud Computing

Cloud computing is a figuring worldview, where a vast pool of frameworks are associated in private or open systems, to give powerfully versatile foundation to application, information and document stockpiling. With the coming of this innovation, the expense of calculation, application facilitating, content stockpiling and conveyance is decreased fundamentally.
Cloud computing is a handy way to deal with experience coordinate money saving advantages and it can possibly change a server farm from a capital-concentrated set up to a variable valued condition.
Cloud figuring depends on an extremely crucial vital of reusability of IT abilities'. The distinction that distributed computing brings contrasted with customary ideas of "matrix registering", "disseminated registering", "utility figuring", or "autonomic processing" is to widen skylines over hierarchical limits.

II. Proposed Method

In proposed work we are work two section one is encryption of video frame and another is decryption of video frame. Proposed work is basically two method is used one is visual cryptography another is Haltone algorithm. d .The most important aim to code transparencies and also the content of every transparency is noise like so secret data cannot be retrieved from anyone transparency via human visual observation or signal.

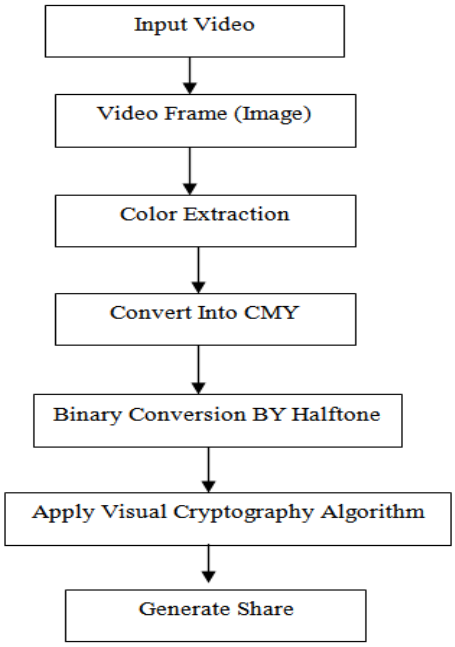


Figure 1: Video Encryption Process

Here also used S-matrix method to design based share object in cryptography method. Figure 1 is show video encryption process. Here initial take video as a input data of system and then design video frame (image) of video. After the video sequence we apply image optimization and color extraction process. After extraction and optimization of data convert one color sequence to another RGB to CMY. CMY is basically rich color of print that is not more affected by noise another region when merge pixel we get original RGB color. After apply Haltone algorithm to design transparency and binary conversion, and then apply Visual Cryptography algorithm to encrypt video sequence and generate share. This share is encrypt data of video.

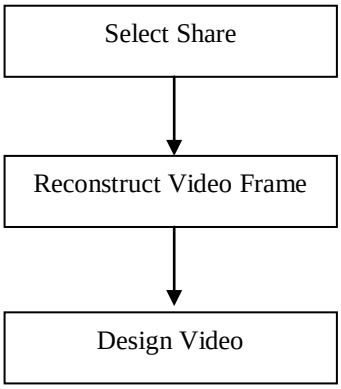


Figure 2: Video Decryption Process

After the encryption we are working decryption process as show in figure 2. Here is select best share and merge to get video frame. Then arrange all frame and design video.

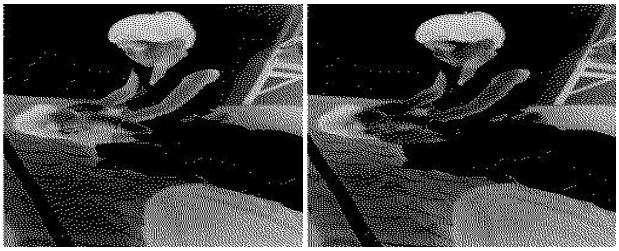
III. Results

Here is take one video. That video is converted frame. Frame is taken as initial object for processing. In this proposed work video frame are encrypted into various shares through MATLAB, so that after compiling specific number of share the original image is visible.

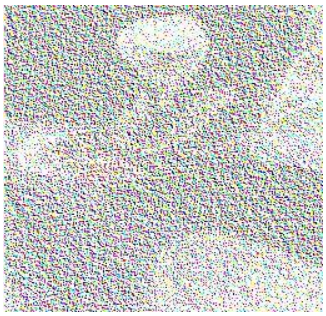
Table 1: Performance analysis of sample image 1 after Gaussian noise module variance.

Performance	**R**	**G**	**B**
MSE	**1.7092e+03**	1.6956e+03	1.6293e+03
PSNR(in DB)	31.6056	31.6751	32.0217

After encryption the performance analysis is done with the help of PSNR and MSE values.



(A)



(B)

(A) Input Image (B) Result

Figure 3. Proposed result

IV. Conclusion

In the proposed work cryptography is done on the three sample images by applying floyed dithering halftone technique. Four shares are created which acts like noise on the transmission media when they are transmitted separately but on superimposing these shares the original sample images can be seen. For the performance analysis the two parameters are considered which are PSNR and MSE.All the three images are tested on the same performance parameters in the presence of noises like Gaussian, salt & pepper and speckle noise module. Finally it is observed that the image quality is highly degraded in Gaussian noise module and least degraded in the presence of speckle noise module. The cryptography is done on the colored image hence the three primary color size, red green and blue shows different behavior in different images. In the presence of noise modules .the value of PSNR is higher for red colour in image 1whereas for Image 2 it is least. Similarly the value of PSNR is higher for green and least for red. Hence it can be concluded that the performance of PSNR is independent of the type of noise for RGB component.

References

[1] Y. Kan, et al. “Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach” IEEE Trans. on Multi. 18.5 (2016): 940-950.
[2] P. Vilma, et al. “Dynamic visual cryptography for optical assessment of chaotic oscillations” Opt. & Laser Tech. 57 (2014): 129-135.
[3] Bahrami, Zhila, and Fardin Akhlaghian Tab. “A new robust video watermarking algorithm based on SURF features and block classification” Mult. Tools and App. (2016): 1-19.

[4] N. Bharot,P.Verma,S. SharmaDistributed denial-of-service attack detection and mitigation using feature selection and intensive care request processing unit Arabian Journal for Science and Engineering 43 (2), 959-967
[5] Pandey, Anjney, and Subhranil Som. "Applications and usage of visual cryptography: A review" Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), 2016 5th International Conference on. IEEE, 2016.
[6] Laxminarayan Gahalod, Sanjeev Kumar Gupta, "Performance of Digital Image Watermarking using Level-1 DWT", International Journal of Research Culture Society ISSN: 2456-6683 Volume 2, Issue-4, April (2018).
[7] Ma, Zhaofeng, et al. "A Novel Image Digital Rights Management Scheme with High-Level Security, Usage Control and Traceability" Chinese Journal of Electronics 25.3 (2016): 481-494.
[8] Chai, Xiuli, Kang Yang, and Zhihua Gan. "A new chaos-based image encryption algorithm with dynamic key selection mechanisms" Multimedia Tools and Applications : 1-21. (2016)
[9] Nitesh Bharot, Sanjeev Kumar Gupta, "Mitigating Distributed Denial of Service Attack in Cloud Computing Environment using Threshold based Technique", Indian Journal of Science & Engineering Volume- 9 Issue- 38, October- 2016.
[10] Nitesh Bharot, Sanjeev Kumar Gupta, "(DDoS Attack Detection and Clustering of Attack and non-Attacked VM's using SOM in Cloud Network)", International Conference on Advanced in Computing and Data Sciences (ICACDS-2019)
[11] Pritaj Yadav,Sitesh kumar Sinha,S. Veenadhari "Two-Party Password Authentication Key Exchange Protocol using OTPK" accepted for publication in Journal of Emerging Technologies and Innovative Research (JETIR) Vol.6, Issue 1, January-2019.
[12] Bharti Chourasia, Dr Sanjeev Kumar Gupta & Anshuj Jain; Performance analysis of multi level threshold based OTSU method: Internation Journal of Advance Research and Innovative Ideas in Education (IJARIIE) e-ISSN: 2395-4396; Vol.2 Issue 6 2016; DUI: 16.0415/IJARIIE-3473.
[13] Hofmeister T., Krause M., and Simon H. U. "Contrast-optimal out of secret sharing schemes in visual cryptography" Compute. Sci., vol. 240, no. 2, pp. 471–485, Jun. (2000)
[14] P. A. Eisen and D. R. Stinson "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels" Designs Cryptography, vol. 25, no. 1, pp. 15–61, (2002)
[15] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images" WSCG J., vol. 10, no. 2, pp. 303–310, (2002)
[16] H. Koga "A general formula of the -threshold visual secret sharing scheme" in Proc. Int. Theory and Application of Cryptology and Information Security: Advances in Cryptology, Dec., pp. 328–345. (2002)
[17] Laxminarayan Gahalod, Sanjeev Kumar Gupta, "A Review on Digital Image Watermaking using 3-Level Discrete Wavelet Transform", (IJSRSET) ISSN: 2394-4099 (Online) ISSN: 2395-1990 (Print) Volume 4, Issue-1, Jan-Fab-(2018).
[18] Girraj Prasad Rathor & Sanjeev Gupta "Enhancement of Fusion using Adaptive Fuzzy Logic on Multi Sensor Images" International Journal for Scientific Research & Development (IJSRD) Vol.5,Issue 01, 2017|ISSn (online) : 2321-061
[19] 4. P. Paulius, and M.Ragulskis. "Image communication scheme based on dynamic visual cryptography and computer generated holography" Opt. Comm. 335 (2015): 161-167.
[20] Yuan, Lifeng, et al. "Secret Image Sharing Scheme with Threshold Changeable Capability" Mathematical Problems in Engineering 2016 (2016).
[21] Laxminarayan Gahalod, Sanjeev Kumar Gupta, "Performance Evaluation of Digital Image Watermarking Using Level 3 DWT", International Journal of Electronics Engineering ISSN: 0973-7383 Volume 11, Issue-1, pp. 113-118 January-2019, June-2019