International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 09, September-2015

Frame Scrambling Algorithm for Video Surveillance Systems

D. Sathya Srinivas,
Research Scholar ,
Department of Computer Applications,
Karpagam University,
Coimbatore, India

Dr. S. Veni,
Research Supervisior,
Department of Computer Science,
Karpagam University,
Coimbatore, India

Abstract **- In the recent years the increasing demand for security has proportionately pushed up the widespread use of digital video surveillance systems. The video surveillance system in use in strategic places such as the public transportation, airports, city centres, or residential areas has increased the safety and security of people or property in the monitored areas.The general public are becoming increasingly worried about theerosion of their rights of privacy.Moreover, the storage systems in which the data is stored rely on the untrusted server for data integrity and access control. Moreover, the server often does not guarantee data integrity and only implements access control. As hackers nowadays are able to manipulate the system and get access to sensitive data stored in a server security guarantees such as integrity and authenticity have become more relevant not only for the server but also for data stored in the server. If integrity is not protected, a hacker could modify video data in a way that intentionally damages the reputation of persons. A solution to a hacker intrusion into the visual privacy is encryption of objects that reveal identities and still allow decryption for legitimate security needs at any time in the future. In this paper, the researchers propose an algorithm based on graph coloring technique to scramble frame sequences and the content of frames in video surveillance videos. The proposed model has been implemented and tested with cat, visiontraffic and canteen videos. The results of experiments show that the entire content of frames can be distorted and thus,make indecipherable while providing with a good level of security. Furthermore, the proposed algorithm does not require any algorithm to identify the region of interest and video inpainting algorithm to erase privacy information from video.**

Keywords*: Privacy protection, video surveillance, pixelization, warping, deidentification*

I. INTRODUCTION

Video surveillance systems are usually installed to increase the safety and security of people or property, prevent robbery, vandalism, shoplifting, booth capturing, or terrorism in the monitored areas[3,8]. But the digital video surveillance systems, especially in public spaces and communities, poses a threat to the human rights, to privacy, and fundamental individual freedoms which has significantly increased the concern for protection of individual privacy[22,23,24]. Therefore, there is a strong demand for solutions which specifically focus on protection of privacy in video surveillance systems.As it is very hard to find an acceptable balance between privacy of public under surveillance and the surveillance tasks at hand,visual privacy protection systems are designed toretain basic characteristics or integrity of visual data and remove personal information. Simple privacy protection methods like blurring, pixelization, and masking are not reversible and insecure; encryption-basedmethods, proposed in [4]are secure but destroy integrity of the original pixel dataand anonymization method in [6]is often complex and require the original data to bestored separately.Similarly,the process of face or object detection, tracking and masking it are the overheads found in k-same, k-same-select, and object replacement techniques. To address these problems,the researchers propose a graph coloring transformation for protection of visual privacy. The proposed scheme represents an encryption method which uses a key to jumble the order of frames of the input video. These scrambled frame-sequences hold video information and these are not in the correct sequence but the contents of individual frames are meaningful. In order to hide the contentsof individual frames, pixels in them are scrambled which destroy visual details and relationships between neighbouring pixels in the frames. Thusthe balance between privacy protection and surveillance task is achieved. The proposed method also ensures secured distribution and storage, while retaining the ability to reconstruct the original data in case of a legal requirement.

The organization of the rest of the paper is as follows: Section 2 gives a brief introduction of the existing encryption methods for privacy protection in surveillance video and their limitations. Section 3 and section 4 present the proposed algorithm and the experimental results. Finally, section 5 concludes the paper with a summary and a discussion of the future work.

II. RELATED WORK

In the recent years, with the development of internet and multimedia technology, multimedia data, especially image, audio and video data, is transmitted in large volume over the insecure internet. These multimedia data are to be protected by providing confidentiality, integrity, and ownership or identity. In this regard, the security of videos has been drawing more and more attention in various applications such as digital television, video-on-demand and video surveillance. Most of the traditional ciphers such

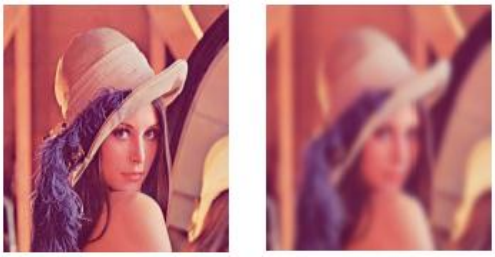
as Data Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), and RSA being used for text or binary data appear not to be ideal for multimedia applications and the reasons are:

- encrypting bulky multimedia data, especially image and video data with the traditional ciphers, is too expensive;
- in the case of digital image, adjacent pixels often have strong correlations, while for video data, consecutive frames are similar and most likely, only few pixels would differ from frame to frame. Such an extremely high data redundancy of multimedia makes the conventional ciphers fail to obscure all visible information;and ,
- traditional ciphers are likely to degrade the data to a perceptually unrecognizable content.

To tackle the above problems, many researchers focused on simple encryption methods like blurring, pixelization, and masking for privacy protection in surveillance video.

A. Blurring

A blurring filter applies a Gaussian function over an image which is presented in Fig.1. This function modifies each pixel of an image using neighbouring pixels. As a result, a blurred image is obtained in which the details of sensitive regions have been removed. Blurring is widely used in Google Street View[9] to modify human faces and number plates.A box blur, also known as "moving average", is a simple linear filter with a square kernel and contains all the kernel coefficients equal. It is the quickest blur algorithm, but it has a drawback, i.e.it lacks smoothness of a Gaussian blur.Algorithm proposed in [4]constructs two blurred video streams. One video stream is publicly accessible where access to some subsets of the least significant bits is restricted. The second stream will have a full bit resolution and is restricted to users with high clearance and is effectively private. This scheme is, therefore, characterized by a public/private encryption/decryption pair and can be extended to implement a scheme that has more than two levels of security.



(a) Original image (b) Blurred image

Fig. 1: Blurring

B. Pixelation technique

The privacy information in the video has to be identified and needs to be obfuscatedfor privacy protection. There are a large variety of such video obfuscationtechniques, ranging from the use of pixelation in [12, 17]to complete object replacement or removal in **[**5,28].The pixelationtechnique decreases the number of pixels in a portion of an image, by replacing the original, smaller pixels with a limited number of relatively large pixelswhich is presented in Fig.2. The luminance of each new pixel is equal to the average luminance of the original pixel that it replaces. This technique removes high spatial frequencies from the image and, at the same time, introduces spurious frequency noise.

In[6]it ismentioned that even highly degraded pictures of faces, as generated by the so-called 'pixelation', provide the participants with enough facial cues to reliably assess features of the pixelized persons. Lander et al. conducted experiments to investigate the effectiveness of pixelation and blurring. In these experiments, images of frontal viewpoint of head and shoulders of familiar and unfamiliar people who had to be identified were screened to the participants. In their pixelation experiment, masking was achieved by reducing the resolution of the appropriate face. In the second experiment the faces get blurred instead of pixelated. The results of these experiments revealed that participants identified, on an average, 55% and 78% of the familiar people,in the cases where the resolution of the appropriate face area was reduced to 10 pixels/face and 20 pixels/face respectively. On an average participant identified 65% of the familiar people. The reason for the high level of identification (65%)is likely to be a reflection of the additional cues like beard, hair style, and glasses that were available in both our moving and static images. Pixelation has been found to be inadequate in fully protecting a person's identity [25].

(a) Original image (b) Image after pixelation

Fig.2: Pixelation

C. Face deidentification

Video surveillance installed on the roads, offices, supermarkets, parking lots, airports, or any other commercial establishment watch you in your private moments, locate you at a specific place and time or with a person, spy on your everyday activities, or even implicitly control some of your actions. As video surveillance system cannot be avoided in the foresaid locations, one would like surveillance systems obfuscate videos, without revealing any personal information. Traditionally, confidentiality of the data is achieved through encryption. However,

encryption destroys any structure present in the data, thus negating the ability to perform any meaningful video processing task. In order to preserve privacy [7],it is proposed to have a selective scrambling based on solution, [5] face swapping and [10, 13,16] face deidentification and object replacement techniques.

Face obfuscation or masking is the traditional approach to privacy protection where the face region needs to be manually marked and replaced by an elliptical or rectangular overlay, or by pixelation of the area in each video frame. This process is time consuming because, for a few minutes of video, more than ten thousand images have to be inspected, and is unusable in applications such as 24-hour video surveillance, where the amount of data is enormous. The solution is the automatic face deidentification in videos. The process of automatic face de-identification in videos combines face detection, face tracking and face masking. The first step in face de-identification for video is face detection.

There are two approaches to face detection: the feature-based approach and the imagebased approach. Face tracking is a process of locating a moving human face (or multiple human faces) in a sequence of frames. Besides this, face tracking needs to find the same face (in the case of multiple human faces) in a video, predict a face (or multiple human faces) location in the next image frame based on the motion model or the information obtained from the previous consecutive frames. The effectiveness of the face detection and tracking is very important because the face has to be detected and de-identified in each frame of the videos. Each localized and traced face region in each frame has to be de-identified by masking. Some approaches to face masking for privacy protection in video-surveillance systems follow techniques that are used in still-face images using a "black-box" approach, simple blurring filters, and pixelation. An alternative approach to face de-identification, especially popular in the video-surveillance domain, is based on distortion applied to the face image by using transform domain scrambling methods.

D. Object replacement technique

Object replacement techniques replace sensitive information such as human facesor bodies with generic faces [16] or stick figures [3] for privacy protection. These techniques require precise position and pose tracking. Object removal algorithms [6, 9]produce more reasonable and efficient solution for full privacy protection when compared with the results of pixelization.In masking of moving objects [13, 6], individuals, shadows cast by individuals,and background movementsare masked. The main challenge to this approachlies in recreating objects and motion after the removal of private information. The filling of holes created by object removal is accomplishedthrough inpainting[1, 2, 14, 15]which is presented in Fig.3.TheSpace-Time video completion scheme attempts to fill the hole by samplingspatio-temporal patches from the existing video. The exhaustive search strategy usedto find the appropriate patches makes it very computationally intensive. Patwardhanet al. extend the idea of prioritizing structures in image inpainting in [11] tovideo [19].Inpainting techniques that make use of the motion information alongwith texture synthesis and color re-sampling have been proposed in [26, 27, 28]. However, the disadvantage of this method is that the masking of all movement of objects including the background movement, shadows and highlights often result in the masking of most of the images, even though only a small portion is actual identity information.

(a) Original image (b) Image afterremoving theperson and applying Inpainting to filling the hole left behind by the removed object

Fig. 3.Inpainting

E. Warping

In [18] the authors proposed a geometrical transformation called warpingwhich is presented in Fig.4. Pixels in the protected region can be shifted to slightly different locations, thus destroying visual details and relationships between neighbouring pixels of an image. Hence, the balance between privacy protection and surveillance task is transformed into how much the pixels in an image are warped.

Fig. 4. Warped image

F. Scrambling

A study by Dufaux and Ebrahimi[12] indicates that scrambling is superior to simple approaches such as pixelation and blurring.

Scrambling is one of the simplest forms of encryption that can be applied to multimedia data. It usually refers to encryption methods which perform random permutations to video data using some scheme. The histogram of image generally remains the same except for the fact that the individual positions are shuffled. Scrambling is often used as an easy way to encrypt live analog/digital video signals such as surveillance camera feeds where heavy ciphers are ruled out because of computational delay. Some of the most common techniques include:

- Line Inversion Video scrambling: This technique inverts the whole or some parts of the signal scan lines. This approach is relatively cheap and simple to implement but the security level achieved is low.
- Sync Suppression Video scrambling: In this technique the horizontal/vertical line syncs are hidden or entirely removed. This provides a low-cost solution to Encryption and provides good quality video decoding. A typical disadvantage is that the level of obscurity reached by this scheme depends on video content.
- Line Shuffle Video scrambling: In this scheme each signal line is re-ordered. Although this scheme provides reasonable security, it requires a lot of storage to re-order the screen.
- Cut and Rotate Video scrambling: In this approach, each scan line is cut into pieces and then re-assembled in a permuted manner. This scheme provides a compatible video signal, and gives an excellent amount of obscurity and stability. However, it requires specialized scrambling equipment.

The main advantages of the scrambling based privacy protection techniques are that they are reversible. By knowing a secret key, which could be stored and transmitted securely, one can decode the video back to undistorted state. Another advantage is that scrambling based techniques require less processing power.

III. PROPOSED ALGORITHM

The proposed algorithm is implemented in three phases.

A. Constructing MxNFRAMES matrix of frame numbers.

In [21] image **I** is partitionedintoblocks and the order in which the blocks are chosen for scrambling is stored in 1st column of **BlockTraversal**matrix. In this work,instead of an image**I,MxNFrames** matrix which stores the frame numbers(1 to f_n) is partitioned into **MxN**blocks. The number of rows **M** and the number of columns **N** in **MxNFrames** matrix is decided by the user involved in encrypting the surveillance videos. Therefore, a surveillance video is treated as collections of **P**partitions of **M** rows and **N** columns. If we are not able to arrive at **P** partitions of equal sizes, then the (P+1)th partition may be of different size. The proposed algorithm takes partition after partition and scrambles the order of the sequences of frames in the selected partition. **M** and **N** form a part of the secret key. If correct value of **M** and **N**is not used at the decryption end, the sequence of the frames in the decrypted video will not be in order.

B. *Scrambling the order of frames*

Algorithm in [20] is followed to construct **COLOR_PAD** matrix where 15 colour codes are arranged in a **12x6COLOR_PAD** matrix. The colour codes in **COLOR_PAD** are arranged in such a way that, for any colour code $\mathbf{C_i}$, none of its 16 neighbours along its diagonal is coloured by $\mathbf{C_i}$.**BlockTraversal**$_1$matrix of f_n rows and 2 columns is constructed as explained in image partitioning phase in [20].$f_n$represents the number of frames in a given surveillance video. The **1st** column of**BlockTraversal**$_1$records the random order in which the frames will be picked from the input video and placed in the output video or the encrypted video and the **2nd**column records the color code assigned to theframe. Fig.5 shows the first 8 frames after scrambling the sequence of frames of input video visiontraffic.

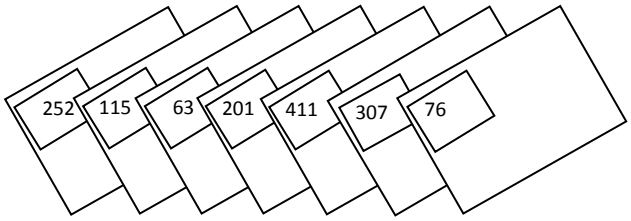


Fig. 5 : First 8 frames from the 531 frames of scrambled video of visiontraffic

C. *Scrambling the content of the frames*

Mere scrambling the order of the frames does not guarantee privacy protection. The sensitive object or context associated with the sensitive object in the frames remains undisturbed. Object replacement techniques are used to remove the sensitive static or moving objects in order to implement privacy protection. But, it requires precise position and pose tracking techniques. Moreover, it also leads to an additional process, video inpainting, to fill the holes left by the sensitiveobjects removed. Object replacement techniques followed by video inpaintingdoes not stop with just replacing the sensitive objects but also replaces the context information associated with the sensitive object which leaves a small part of the image undistributed. The main challenge to this approach lies in recreating objects and motion after the removal of private information. To avoid the replacement techniques and video inpainting and to make the recreating of objects easy, the content of the frame is scrambled in the proposed algorithm.

BlockTraversaland **ScrambleIndex**are constructed as explained in image partitioning and scrambleindex constructing phases in[21]. The functions in Table 1 are used in scrambling the sequence of the frames and the content of frames.

Table 1: The name of the function and the description of the work carried out by them

Function Name	Description
ScrambleFrame($frame_i$)	scramble the content of red component, green component and blue component matrices offrame f_i using the scrambling process in [21]
Reset(*ScrambleIndex*)	The content of Column 1 & Column 3 of scrambleindex is also placed in its Column 2 and Column 4
ReadFrame($frame_i$)	reads frame $frame_i$from the $input_{video}$ videoand returns red component, green component and blue component of $frame_i$
WriteFrame($frame_i$)	Writesthe red component, green component andBlue component in $frame_i$ to $output_{video}$
Numframes($input_{video}$)	returns the number of frames in the $input_{video}$
ChangePixelVal($f\ (r,c)$)	Changes the value in (r,c) of matrix f. $f$may represent red component or green component or Blue component matrix. The one time pad generated by algorithm is used to change pixel value.

The process of scrambling the order of the frames and its content is performed as shown in Fig.6 andFig.7.By default the content of a frame is scrambled only once. Moreover, if the user wishes to scramble the content of the frame more than once then we have limited the number of times to the square root value of one of the color code in the color pad. The number of times the content of the frame is to be scrambled also forms a part of the secret key.

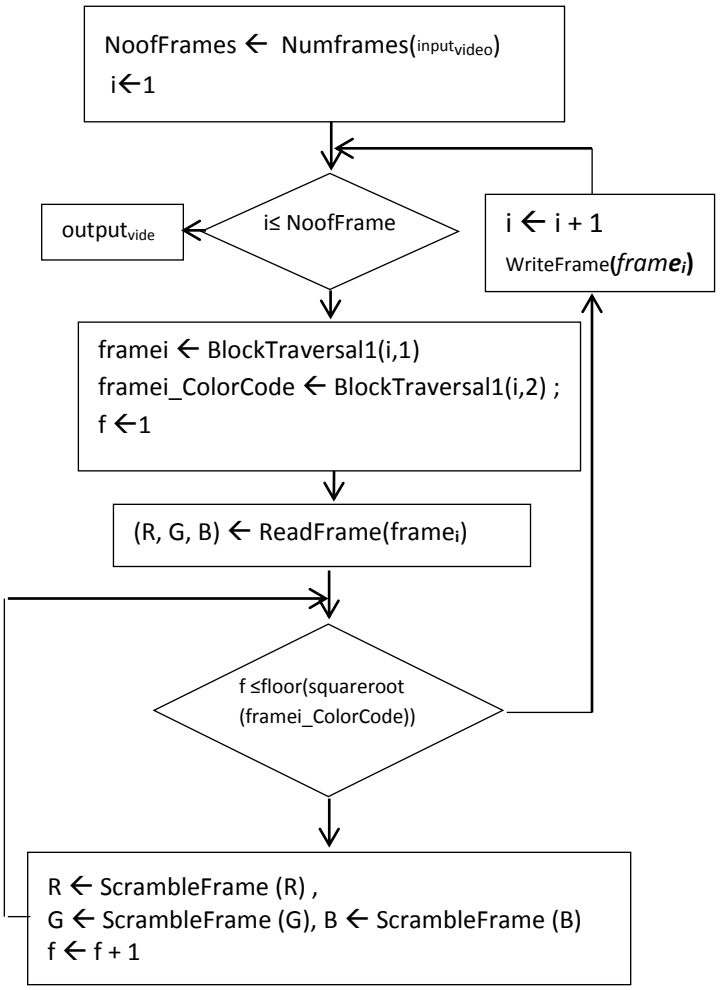


Fig 6: Video frames order scrambling process

The histogram of a frame before scrambling and after scrambling the pixel positions remains the same which reveals the fact that the change in the position of pixels does not bring any change in the histogram. This may give a lead to an unauthorized user about the procedure used in the scrambling of the pixels.Hence it is necessary to change values of the pixels of the scrambled frame so that the histogram of the original image and that of the scrambled image are totally different.

A video is simply made up of picture or still shot or an image called as frame. 25 to 30 frames are run in succession in a second to produce what appears to be a seamless piece of film or video. Each frame can be selected on its own to print out as a single photograph. Hence the

procedure proposed in [21] to change the pixel values in an image is used to change values of the pixels in a frame.

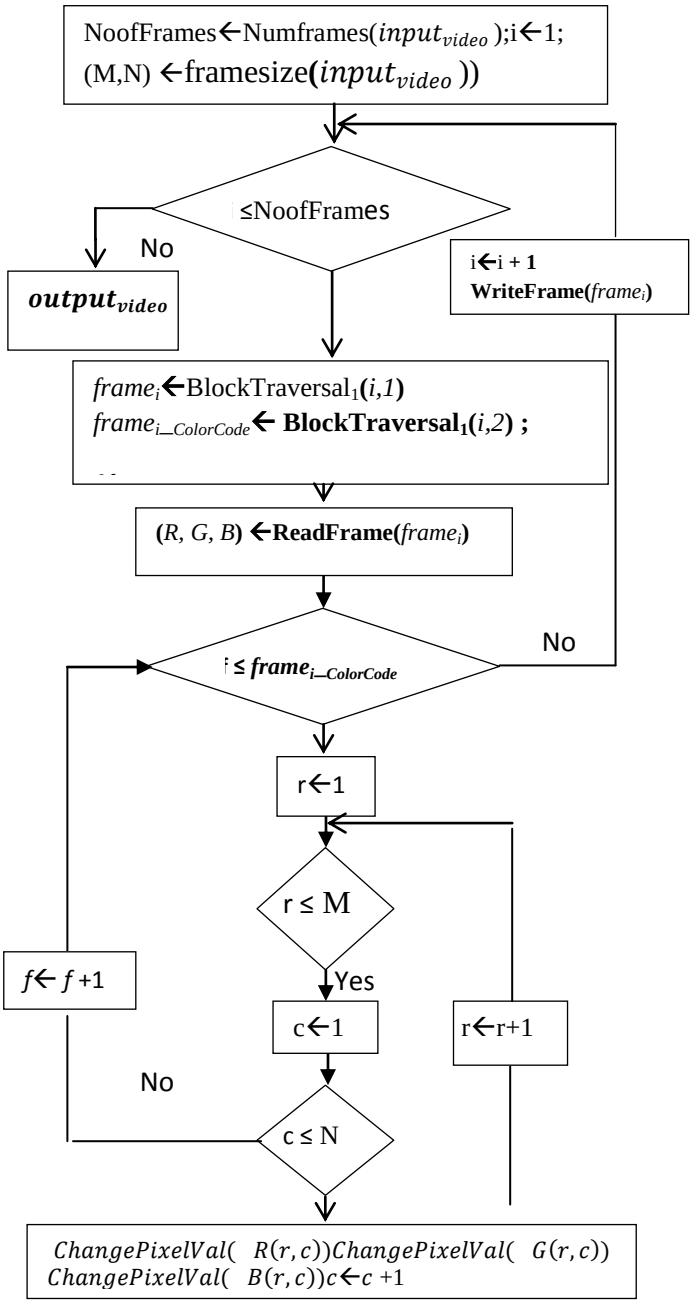


Fig. 7: Changing the pixel values of video frames

IV. EXPERIMENTAL ANALYSIS

The simulator for the proposed algorithm is implemented using MATLAB version 7.12.0.635 (R2011a). The performance is measured on a 2.6 GHz Pentium Core 2 Duo system with 4 GB RAM running Windows 7. The proposed technique is applied on surveillance videos: visiontraffic, canteen and cat. 8 different cases were analysed to test the performance of the proposed technique.

A . Scrambling for Privacy

The 512 frames visiontraffic video was partitioned into two partitions of 256 frames in each. First, the order of the frames was shuffled or scrambled and stored. Then, the original video is removed. The first 4 frames in scrambled video of visiontraffic are shown in Fig. 8. The numeric values in the frames represent the frame numbers.

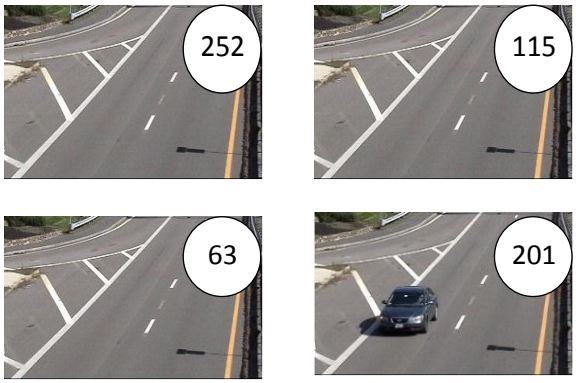


Fig. 8: First 4 frames chosen from the scrambled frames of visiontraffic surveillance video

Next the pixel positions in the frames are scrambled and then their values are changed to hide the information in the frames and it is shown in Fig. 9. As can be observed, the scrambling makes it impossible to identify the content of the frame. This technique is therefore suitable to preserve privacy in video surveillance system.

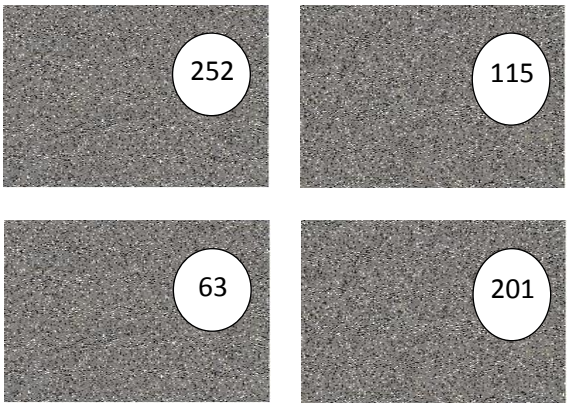


Fig. 9: content of the frames inFigure8 after the pixel values are changed in them is changed

B . Key sensitivity analysis

The encryption system should be sensitive to the small changes on the decrypted keys. And, generate a wrong decrypted image, if there is a small difference in the decryption keys. Keys **13579 71 55 47 58 03 12 17 15 13 19362 128 03 15 05 14 13 117 211 121 87 55 72 14 02** wereused to scramble the order of the frames and change pixel positions and its values in all the frames. The scrambled content of the frames inFig. 8 is shown in Fig. 9. To validate the security of the proposed scheme, the frames in Fig.9 are decrypted bypartition size as 14x14

instead of 16x16 andby choosing a wrong(a) seed value for generating color codes, (b) color pattern which, in turn, has changed orientation which is totally different fro. the one used in the encryption process, (c) seed value for generating the order in which the blocks are to be accessed, (d) prediction of number of blocks of group 1,(e) prediction of either total number of rows or columns of a block, (f) sequence of blocks of group 1, (g) filling pattern, (h) row in pixel_value matrix,(i) column in pixel_value matrix, (j) row in PMGR, (k) row in PMGG,(l) row in PMGB, and (m) direction combination.Fig.10 shows the content of the frame 401 when decrypted using a wrong decryption keys.

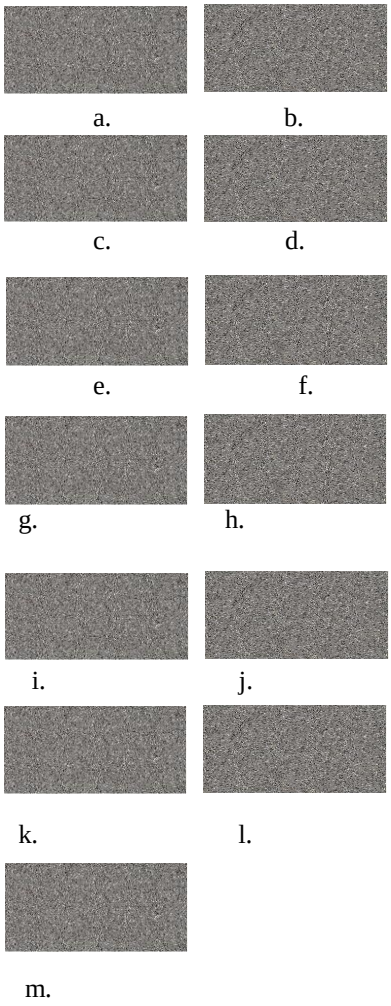


Fig.10: Content of frame 401 when decrypted with wrong keys

C. Time Analysis

To evaluate the performance of this algorithm,visiontraffic video of 512 frames length and a running time of 17 seconds was used. The video is split into smaller partitions of MxN frames each. The frames are shuffled. The content of the frames is completely changed. The table 2 below shows the time in seconds spent on each stage. All these computations were done on a standard computer. Decryption took exactly the same amount of time as it was in just the reverse process. Although the encryption time is higher than the total running time of the video, the type of data protection it provides is unmatchable.

Table 2: Encryption time

Video	Frame size	No.of frames	Size in MB	Frame rate	Running time of original video in seconds	Encryption time in seconds	
						scrambling the content of the frames	Changing the order of the frames
Visiontraffic	675x360	531	14.9	30	17	16.5672	26.2660
Competition	720x495	426	15.0	30	14	13.5912	29.0055
Cat	180x135	241	1.10	30	08	07.8939	14.4416

V. CONCLUSION

In this paper, graph coloring technique is employed to scramble the order of the frames as well as the pixel values of the frames. Simulation results show that the proposed scrambling can be applied to hide the content of the frames. Finally, the method provides a good security level. Currently, the researchers are working further to modify the scheme to adjust with the structure of frames of movie files.

REFERENCES

1. M. Bertalmio, A. L. Bertozzi, and G. Sapiro, “Navier-stokes, fluid dynamics, and image and video inpainting,” in Proc. IEEE Comput. Vis. Pattern Recognit., 2001, pp. 355–362.
2. Bugeau, M. Bertalmío, V. Caselles, and G. Sapiro, “A comprehensive framework for image inpainting,” IEEE Trans. Image Process., vol. 19, no. 10, pp. 2634–2644, Oct. 2010.
3. D. Chen, Y. Chang, R. Yan, and J. Yang. “Tools for protecting the privacy of specific individuals in video,” EURASIP Journal on Advances in Signal Processing, 2007:Article ID 75427, 9 pages, 2007.
4. Christopher Thorpe, Feng Li, Zijia Li, Zhan Yu, David Saunders, and Jingyi Yu , “A Coprime Blur Scheme for Data Security in Video Surveillance,” IEEE Transactions on pattern analysis and machine intelligence, vol. 35, no. 12, December 2013 3066-72
5. Criminisi, A., Perez, P., Toyama, K, ” Region filling and object removal by examplar based image inpainting,” IEEE Transactions On Image Processing Vol. 13 No. 9 (2004) 1200–1212.
6. Dufaux, F., &Ebrahimi, T. (2010). “A framework for the validation of privacy protection solutions in video surveillance,” In Multimedia and Expo (ICME), 2010 IEEE International Conference on (pp. 66–
7. Dufaux, F., Ouaret, M., Abdeljaoued, Y., Navarro, A., Vergnen`egre, F., &Ebrahimi, T. (2006). “Privacy enabling technology for video surveillance. In Mobile Multimedia/ Image Processing for Military and Security Applications,” Proceedings of SPIE (pp. 1–12). volume 6250.
8. F. Dufaux and T. Ebrahimi, “Scrambling for Video Surveillance with Privacy,” in Proceedings of the Conference on Computer Vision and Pattern Recognition Workshop, 2006, pp. 160–166.
9. Frome, G. Cheung, A. Abdulkader, M. Zennaro, B. Wu, A. Bissacco, H. Adam, H. Neven, and L. Vincent. “Largescale Privacy Protection in Google Street View,” In International Conference on Computer Vision, 2009.

10. JiayaJia, Yu-Wing Tai, Tai-Pang Wu, and Chi-Keung Tang. Video repairing under variable illumination using cyclic motions. IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI), 1:364–371, July 2006.
11. Y. T. Jia, S. M. Hu, and R. R. Martin. Video completion using tracking and fragment merging. In Proceedings of Pacific Graphics, volume 21, pages 601–610, 2005.
12. Lander K, Bruce V&Hill H. (2001) "Evaluating the effectiveness of pixelation and blurring on masking the identity of familiar faces ," Applied Cognitive Psychology , 15 , 101 - 116 .
13. O. Le Meur, J. Gautier, and C. Guillemot, "Examplar-based inpainting based on local geometry," in Proc. 18th IEEE Int. Conf. Image Process., Sep. 2011, pp. 3401–3404.
14. O. Le Meur, M. Ebdelli, and C. Guillemot, "Hierarchical Super Resolution-Based Inpainting," IEEE Transactions on image processing, vol. 22, no. 10, October 2013.
15. Neustaedter C., Greenberg S., Boyle M., Blur filtration fails to preserve privacy for home-based video conferencing. ACM Transactions on Computer Human Interactions (TOCHI) (2005) in press.
16. E. N. Newton, LatanyaSweeney , and B. Main. Preserving privacy by de-identifying face images. IEEE transactions on Knowledge and Data Engineering, 17(2):232–243, February 2005
17. Nurmoja M. ,Eamets T. , Harma H-L. , & Bachmann T. (2012) Dependence of the appearance-based perception of criminality, suggestibility, and trustworthiness on the level of pixelation of facial images . Perceptual & Motor Skills , 115 , 465 - 480 .
18. Pavel Korshunov and TouradjEbrahimi, "Using Warping for Privacy Protection in Video Surveillance," Multimedia Signal Processing Group, EPFL, Lausanne, Switzerland
19. K. A. Patwardhan, G. Sapiro, and M. Bertalmio. Video inpainting under constrained camera motion. IEEE Transactions On Image Processing, 16(2):545–553, Feb 2007.
20. SathyaSrinivas.D., Veni.S. Novel Image Scrambling Algorithm using Graph Coloring International Journal of Applied Engineering Research Volume 10, Number 15 (2015) pp 35131-35149
21. SathyaSrinivas.D., Veni.S. Image Encryption Algorithm Based on Graph Coloring. International Journal of Applied Engineering Research
22. J. Schiff, M. Meingast, D. Mulligan, S. Sastry, and K. Goldberg. Respectful cameras: Detecting visual markers in real-time to address privacy concerns. In International Conference on Intelligent Robots and Systems (IROS), 2007.
23. TakaakiShiratori, Yasuyuki Matsushita, Sing Bing Kang, and Xiaoou Tang. Video completion by motion field transfer. In Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), volume 1, pages 411–418, June 2006.
24. J. Wickramasuri et.al, "Privacy protecting data collection in media spaces," ACM Multimedia, pages 48–55, October 2004.
25. W. Zhang, S.-C. Cheung, and M. Chen.,"Hiding privacy information in video surveillance system," In Proceedings of the 12th IEEE International Conference on Image Processing, Genova, Italy, September 2005.
26. Xu, Z., Sun, J., " Image inpainting by patch propagation using patch sparsity," IEEE TIP 19 (2010) 1153–1165
27. Yonatan Wexler, Eli Shechtman, and Michal Irani. Space-time completion of video. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(3):463–476, 2007.
28. Yunjun Zhang, Jiangjian Xiao, and Mubarak Shah. Motion layer based object removal in videos. In Proceedings of the Seventh IEEE Workshops on Application of Computer Vision, volume 1, pages 516–521, 2005.

AUTHOR'S BIOGRAPHY

D. Sathya srinivas obtained his M.Phil from Allagappa University, Karaikudi, India in 2004. His research interests include Data structures, Data Mining, Information Hiding, and Neural Network. He has published several papers in International Journals and more than 15 conferences at National and International level. He is pursuing Ph.D. in Karpagam University.

Dr. S. Veni completed her Ph.D in Computer Science from Bharathiar University in 2014. She is working as Associate Professor in Department of Computer Science, Karpagam University, Coimbatore. Her experience is 12 yrs. she has presented various papers in National and International Conference. Her research interests are Computer Networks