INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Selective Video Encryption using Harmony Search

Jyoti Singh
M. Tech Scholar, Dehradun Institute of Technology, Dehradun, India
Ashok Kumar
Assisant Professor, Dehradun Institute of Technology, Dehradun, India

Abstract:
To prevent video from unauthorized access and fabrication, the video should be encrypted before sending them on the unsecure network. Traditional method of encryption like AES, DES are not suitable for heavy multimedia objects like videos of conferences etc. due to their high computational complexity and restricted size of the key. We propose a methodology of selective encryption of video using keys generated by harmony search a meta-heuristic artificial intelligence technique. We perform selective encryption to reduce encryption time and encrypt on potential confidential information. We compared the efficiency of the algorithm using entropy and found that proposed technique is suitable for video encryption.

Key words: *MATLAB, Harmony Search, Selective encryption, Entropy*

1. Introduction

In today's world there is a huge growth seen in multimedia highway. Large size images are sent over the network. Some of the images contain potential confidential information. Since an image has a fixed resolution of 1024X680 and small in size so it is very easy to decrypt an image. If a sender tries to send multiple images, he has to encrypt them separately which might generate similarity in pattern for eavesdropper [4]. If a sequence of images differs in small position then it is better to convert the sequence of images into videos and then encrypt. The images sent over network are not only grayscale, binary but coloured which change their dimension from 2D to 3D [6]. The video encryption finds its importance in military communication, confidential video conferences, remote sensing videos which contain potential information about the landscape of the country [3]. Traditional methods exist for video encryption which can be categorised as Block Cipher cryptographic algorithm like AES, DES and artificial intelligence cryptographic algorithm which are not limited by the length of the key like Ant Colony cryptosystem, Genetic Algorithm cryptosystem which are heuristics based. Falling into the category of artificial intelligence is Harmony search algorithm and more similar to genetic algorithm but much efficient than other Artificial Intelligence (AI) techniques [4]. Harmony search is a relatively new meta-heuristic algorithm for continuous optimization, in which its concept initiates the process of music improvisation. We proposed the process of selective encryption because of the explosion of networks and the huge amount of content transmitted along therefore it increase the size of the data sent, our main goal is the object of consideration in the image or video, hence encryption the object is important irrespective of the environment. The technique of selective encryption not only reduces the size of the encrypted data to be sent but also reduces the time to perform encryption of the video irrespective of its size[1]. The remainder of the article is organized as follows. In Section 2 a brief introduction of all the research done in field of encryption of images, videos. In Section 3 a brief introduction to harmony search with its algorithm modified for video encryption and a brief introduction to selective encryption. In Section 4, we discuss about the simulation environment and results. In section 5, we provide the conclusion of our research.

2. Literature Survey

Adnan M. Alattar, proposed selective encryption methods for MPEG-II, MPEG-IV, H.261 and H.263+. He stated that encrypted I-macro block of video requires half the processing time. He stated that the method showed 60-82% reduction in processing time. Wenjun Zeng proposed the method of joint encryption and compression of the video in the frequency domain by selecting bits in the frequency domain. This method is suitable for relative small scale video, but not suitable for remote sensed images where the images details are very minute. Yong Wang proposed a new chaos-based fast image encryption where the image is partitioned into blocks, shuffled and encrypted using pseudorandom numbers from spatial-temporal chaos. A. Nag divided the image into 2X2pixels blocks and each block is encrypted using XOR operation by 64 bit key which might be strong enough for small scale images and low processing system but when it comes to AVI files and high detailed images we can't create a clean demarcation in the image.

GauravBhatnagar proposed a scheme to scramble pixels positions using Saw-tooth space filling curve followed by selection of pixels of interest and the diffusion is created using chaotic map.

3. Background

This section provides a brief introduction of every methodology used to carry out the research work. A brief overview of the technique is essential for analysing rest of the research.

3.1. Harmony Search

Geem [1] proposed and implemented Harmony Search, a meta-heuristic algorithm that utilized musical process concept for searching a perfect state of harmony. Harmony search keeps the possible candidate solution, which are initialized randomly within the search space as follows:

For i=0 to Harmony Memory Size (HMS)

For d=0 to Decision variable of the problem domain

Candidate (d) =LB (d) + (UB (d)-LB (d)) x rand ()

Where LB (d) and UB (d) are the lower an upper bounds in the search space and rand () function delivers a random value between 0 and 1. This algorithm is an improvisation process of pitch value to bring search to optimal solutions. There are three main parameters controlling the improvisation process, that are harmony consideration rate (HMCR), pitch adjustment rate (PAR) and the bandwidth (bw). In each iteration rand () value is tested against HMCR, if less than candidate solution is generated with memory consideration otherwise by random selection. The candidate generated by memory consideration is further adjusted by pitch adjustment rate. [2] The final candidate solution generated after d iterations is tested for fitness. If the fitness value of the candidate is higher than the previous candidate then new candidate is taken as a solution for further candidate improvement in HMS iterations. The process of harmony search can be related to genetic algorithm process of finding the best candidate solution.

3.1.1. Harmony Search Crossover

Genetic algorithm employs crossover based on crossover probability, with similar nature next element of the candidate vector is selected based on HMCR that is

If rand () < HMCR

Candidate (d) =HM(R (d), d);

Else

Candidate (d) =LB (d) + (UB (d)-LB (d)) x rand ();

End if

3.1.2. Harmony Search Mutation

In genetic algorithm mutation occurs based on some mutation probability threshold. In the process of mutation changes are made in the candidate solution to make it more fit, similarly the pitch adjustment rate behave as mutation probability and the candidate solution is mutated using bandwidth of sound.

If rand () <Pitch Adjustment rate then

Candidate (d) =candidate (d) +rand () x Bandwidth

End if

```
Set parameters: HMCR, HMS, PAR
Initialize HM = {HM0, HM1, HM2… HMHMS-1}
i← 0
while i < MAXITERATIONs do
for d=0 to D-1 do
   if rand() < HMCR then
      candidate(d)=HMR(d) where R=random number generated by poisson formula
         if rand() < PAR // pitch adjustment
            candidate(d)=candidate(d)+ rand() X bw
         end if
   else
   candidate(d) = LB(d) + (UB(d) – LB(d))X rand()
   end if
end for
for k=1:length(X dimension)
      P(k)=fitness(candidate(k));
 end
 SumP=sum(P);
 for j=1:length(Y Dimension)
      Q(j)=fitness(HMWorst(j));
 end
SumQ=sum(Q);
 if SumP > SumQ
    HMWorst=candidate;
 end
 i=i+1;
end
hm=HMWorst;
end
```

Figure1: Harmony Search Algorithm

3.2. Selective Encryption

With large amount of data on the network highway requires greater amount of security and bandwidth. Same is true when we send our encrypted file on the insecure network. Encrypting the complete file generates patterns in the encrypted file and also encrypting entire video takes time [5]. Here we are using a technique that encrypted the confidential information in the video and the time taken for encrypting is reduced. [2] The aim of selective encryption is to reduce time while at the same time preserving a sufficient level of security. Selective encryption finds its application in real time networking, high definition delivery, mobile communication etc.

4. Simulation and Results

4.1. Simulation

Selective encryption of video using harmony search was carried out using MATLAB R2011a with video in audio visual format (.avi). The methodology followed during the course of research was generation of pseudorandom random vectors of the length equivalent to Y dimension of the 2D image. The pseudorandom vectors are passed to harmony search routine to select one vector which we call a best candidate solution. The iterations for Harmony search are kept to 10000. The key generated by the harmony search routine is passed as input to the encryption routine of the video. During the process of encryption of video each pixel of the video in encrypted by the key that is a pixel at position (x, y, z) is encrypted by the key for 240X320 iteration (image resolution of our example video) followed by encryption of pixel at position (x,z,y) , at position (y,x,z), at position (y,z,x), at position (z,y,x) and at position (z,x,y)[2] . The resulting parts of the video are combined to demonstrate selective encryption where the environment shows little change whereas the object of consideration blanks out.

S. no	Property	Value
1.	Video file	.AVI
2.	Image resolution	240X320
3.	Maximum Iteration for harmony search	10000
4.	HMWorst	{1……..320 times}
5.	Fitness Function	Permutations and Combination

Table 1: Simulation environment

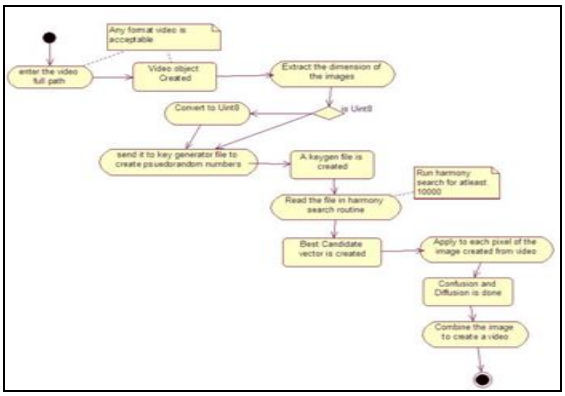

Figure 2: Activity diagram to show the active states in the process of encryption using harmony search.

4.2. Result and Analysis

The main aim of encryption algorithm used for multimedia object is the decrease the correlation between the pixels in the image and increase the entropy of the pixel value so that decryption of the multimedia object is difficult. Entropy of a multimedia object is calculated as

$$H = -\sum_{k=0}^{G-1} P(k)\log_2(P(k))$$

Where: H: entropy, G: grey value of input image (0…255).
P (k): is the probability of the occurrence of the symbol.

S. no.	Image Part in Original Video	Image Part in Encrypted video
1.	0.1663	0.8361
2.	0.1875	0.847s5
3.	0.1712	0.8420
4.	0.1512	0.7802
5	0.1339	0.7732

Table 2: Entropy of original video and encrypted video

The average entropy of the encrypted video clearly shows strong encryption of the video using harmony search generated key.

5. Conclusion

This paper presents a novel methodology of selective encryption of video using harmony search. This methodology provide a valuable tool for secure video transfer over the network. As shown in the result, this technique tremendously increase the entropy of the image frames of the video which makes it difficult decrypt and more secure. This technique has been tested using MPEG format video, AVI format video and MPEG II format video and result was fascinating.

Harmony search is a versatile meta-heuristic algorithm that can be applied in various fields. Changing the HMCR, PAR can further improve the performance of the algorithm. Videos of higher pixels will develop stronger key as the length will be high, large number of permutation and hence more string encryption. In the process of generation of pseudorandom keys if initial key to start is high more robust encryption can be performed as strongest key will be selected by the harmony search. The field of encryption has wider prospects and involvement of artificial intelligence has led to generation of enormously long keys.

6. References

1. A Harmony Search with Adaptive Pitch Adjustment for Continuous Optimization Chukiat Worasucheep Applied Computer Science, Department of Mathematics, Faculty of Science, King Mongkut's University of Technology Thonburi, Bangkok 10140, Thailand
2. Selective image encryption based on pixels of interest and singular value decomposition Gaurav Bhatnagar Corresponding author contact information, E-mail the corresponding author,Q.M. Jonathan Wu.
1. 3.Image encryption using affine transform and XOR operation Nag, A. ; Dept. of Inf. Technol., Acad. of Technol., Bandel, India ; Singh, J.P. ; Khan, S. ; Biswas, S.
2. 4 Applied Soft Computing Volume 11, Issue 1, January 2011, Pages 514–522 Cover image A new chaos-based fast image encryption algorithm Yong Wanga, b, Corresponding author contact information, E-mail the corresponding author, Kwok-Wo Wongb, Xiaofeng Liaoc, Guanrong Chenb
3. 5. Secure Image Data by Double encryption International journal of computer application jayant kushwaha
4. 6. A Lightweight Encryption Algorithm for Images, springer