UNIVERSIDADE FEDERAL DE PERNAMBUCO

GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

CENTRO DE INFORMÁTICA

2012.1

EXTENSÕES PARA UM MÉTODO DE ENCRIPTAÇÃO DE VÍDEOS DIGITAIS BASEADO EM PERMUTAÇÕES

PROPOSTA DE TRABALHO DE GRADUAÇÃO

Aluno: Caio César Sabino Silva (ccss2@cin.ufpe.br)
Orientador: Tsang Ing Ren (tir@cin.ufpe.br)

Recife, Abril de 2012

Contexto

No contexto de aplicações de multimídia, diversos sistemas de vídeo, como videoconferência, prezam bastante pelo requisito de segurança. Para garantir o sigilo das informações nessas aplicações, surgiram diversos métodos de encriptação específicos para vídeo [1], uma vez que a quantidade de informações nesse tipo de mídia é grande. Outra questão importante em encriptação de vídeo é que o dado codificado também seja legível por *decodificadores padrões* sem ocorrer erro, mas não podendo obter diretamente a informação protegida, de modo que o esquema possa ser usado sem a necessidade de alterar os módulos padrões de codificação/decodificação.

Para esse fim, um método existente na literatura [2] propõe a encriptação do vídeo como um passo antes da codificação utilizando técnicas de permutação nos pixels de cada quadro do vídeo para garantir o sigilo da informação a ser codificada. As técnicas de permutação utilizadas nessa técnica tendem a preservar ou melhorar a *correlação espacial* em cada quadro do vídeo, de maneira que o dado codificado final é, em geral, mais compressível quando utilizando um codificador que se baseia apenas na correlação espacial em seu algoritmo de compressão, como Motion PNG, Motion JPEG. O esquema descrito é provadamente seguro contra alguns tipos de ataque, como força bruta e texto puro conhecido/escolhido.

Entretanto, esse método não foca em explorar adequadamente *correlação temporal*, de forma que codecs mais avançados, como *MPEG-4*, perdem parte de seu potencial de compressão quando usam somente essa técnica. Além disso, o esquema não funciona para vídeos codificados com quadros do tipo B (*B frames*), que utilizam o quadro anterior e posterior como forma de minimizar a quantidade de informações a serem expressas no quadro propriamente.

Objetivo

O objetivo deste Trabalho de Graduação é a extensão do esquema de encriptação baseado em permutações mencionado, de maneira a explorar mais adequadamente a correlação temporal do vídeo, para então ter um melhor desempenho em termos de compressão e qualidade de vídeo quando utilizando codecs mais avançados.

A primeira extensão proposta é possibilitar que o método funcione com quadros do tipo de B. Para isso, o esquema do algoritmo precisa ser alterado e é importante garantir que o dado poderá ser codificado/decodificado adequadamente mesmo quando utilizando codecs com/sem perda.

Outra extensão possível é utilizar técnicas de *Motion Estimation* e *Motion Compensation* para estimar movimento de objetos das cenas no próximo quadro e poder transformar as permutações utilizadas no esquema para obter melhor *matching* e possivelmente aumentar a taxa de compressão do esquema.

Por fim, a última extensão propõe o *embaralhamento das cenas* e quadros do vídeo de maneira que o vídeo final tenha um melhor desempenho com a técnica de codificação. Nessa última extensão, a encriptação seria estendida de maneira que o

embaralhamento ocorreria tanto na ordem dos quadros do vídeo, como nos pixels de cada quadro individualmente.

Cronograma

O desenvolvimento deste trabalho está dividido nas seguintes atividades:

Atividades	Março	Abril	Maio	Junho	Julho
Levantamento do estado da arte e definição do escopo do trabalho					
Implementação					
Realização de testes e comparação com o esquema original					
Elaboração do relatório final					
Preparação e defesa					

Possíveis Avaliadores

Os possíveis avaliadores para o trabalho final com as etapas descritas nesta proposta são:

- Tsang Ing Ren
- George Darmiton
- Carlos Alexandre Barros

Assinaturas

Caio César Sabino Silva
Orientando

Tsang Ing Ren
Orientador

Recife, Abril de 2012.

Referências

[1] S. Li, G. Chen, A. Cheung, B. Bhargava, and K.-T. Lo, "On the design of perceptual MPEG-Video encryption algorithms," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 17, no. 2, pp. 214–223, 2005.

[2] D. Socek, H. Kalva, S. Magliveras, O. Marques, D. Culibrk, and B. Furht, A permutation-based correlation-preserving encryption method for digital videos. in Proceedings of the 3rd International Conference on Image Analysis and Recognition (ICIAR '06), vol. 4141 of Lecture Notes in Computer Science, pp. 547–558, Springer, Póvoa de Varzim, Portugal, September 2006.