

ملخص

عملنا في هذه المذكرة يتمحور حول كيفية تطبيق خوارزميات التشفير على الصور الرقمية لأجل ضمان تأمين الصور أثناء الإرسال أو التخزين ضد أي خطر قد يمس محتوى الصورة. التحديين الأساسيين هما: ضمان السرعة في التشفير والفعالية ضد أي هجوم. توجد العديد من التقنيات المختلفة لتأمين الصور، في هذا العمل سنستعمل خوارزمية تشفير هجينة (تناظرية/غير تناظرية) حتى نستفيد من الميزتين الأهم: سرعة التشفير ودرجة أمن عالية. الكلمات المفتاحية: تشفير الصور، التشفير الهجين، السرية

Résumé

Pour assurer la confidentialité des images numériques lors de transmission ou de stockage, on applique les algorithmes cryptographiques. Notre travail s'articule sur l'utilisation ces cryptosystèmes pour sécuriser les images numériques. Les défis principaux dans le chiffrement d'images sont : la performance, c.-à-d. minimiser le temps d'exécution de chiffrement/déchiffrement, et l'efficacité de l'algorithme contre les différentes attaques. Nous choisissons le type de chiffrement hybride, pour profiter des avantages des deux catégories des cryptosystèmes, la vitesse de chiffrement pour le symétrique, et le niveau de sécurité pour le chiffrement à clé publique.

Mots clés : chiffrement des images, cryptosystème hybride, confidentialité.

Abstract

To confirm digital image confidentiality upon transferring or saving, we apply cryptographic algorithms, so our work is dedicated for using those cryptosystems to secure digital images. The principal challenges in coding images are: performance that means to minimize execution time of encryption/decryption, and algorithm efficiency against the different attacks. We use the hybrid encryption type for getting advantages for two categories of cryptosystems, speed of asymmetric encryption, and the level of security for public key encryption.

Keywords: encryption of images, hybrid Encryption, confidentiality