

Intitulé du doctorat : **Imagerie pour systèmes embarqués.**
Epreuve : **Sécurité et compression pour images numériques.**
Coefficient : 03
Durée : 1h30

Questions de Cours : (8 pts)

- ✓ 1. Quelles étapes dans l'algorithme JPEG causent une perte d'information? Citez-les par groupes en différenciant celles qui causent la perte accidentelle due aux erreurs d'arrondi et celles qui la suppriment volontairement. (2 pts)
- ✓ 2. Quelles sont les deux types d'information visuelle que l'algorithme JPEG réduit pour compresser une image en dégradés? (2 pts) *Luminance, chrominance*
- ? 3. Une méthode très simple de vérification d'une éventuelle modification du contenu d'une image est l'utilisation de checksum. Expliquez son principe dans le cas de watermarking aveugle (blind watermarking) ainsi que celui quand le contenu de l'image est pris en compte. (4 pts)

Problème : (12 pts)

On considère l'algorithme de cryptage d'image suivant qui utilise la clé de cryptage $k > 0$.

- Pour la phase diffusion, chaque valeur de pixel est changée selon l'expression: $V_{pn} = \left(E \left(\frac{x+y}{k} \right) \cdot V_p \right) \bmod 256$, où V_{pn} est la nouvelle valeur du pixel et V_p sa valeur actuelle, x et y sont ses coordonnées dans l'image. *mod* est la fonction 'modulo'.
- Pour la phase confusion, chaque pixel change de position dans l'image cryptée selon le principe: $xn = E(x + k \cdot \sin(x))$ et $yn = E(y + k \cdot \sin(y))$ où (xn, yn) sont les nouvelles coordonnées du pixel et (x, y) ses coordonnées actuelles. E la fonction 'partie entière'. Les valeurs du sinus sont considérées en degrés.

- ✓ 1. Dans quelles conditions un pixel ne change pas de positions? Donnez un exemple. (2,5 pts)
- ✓ 2. Dans quelles conditions un pixel ne change pas de valeur? Donnez un exemple. En déduire la forme générale des coordonnées des pixels qui ne changent pas de valeurs. (3 pts)
- ? 3. Pour une image de dimension $N \times M$, calculez la complexité de l'algorithme lorsque les opérations décrites sont exécutés une seule fois sur l'image (négligez le temps d'exécution de la fonction E ainsi que celui de la fonction \sin qui est supposée prendre ses valeurs directement d'une table). (4 pts)
- ✓ 4. Cet algorithme admet-il un algorithme inverse de décryptage des positions? Justifiez votre réponse. (2,5 pts)

Quantification + Down Sample + Conversion