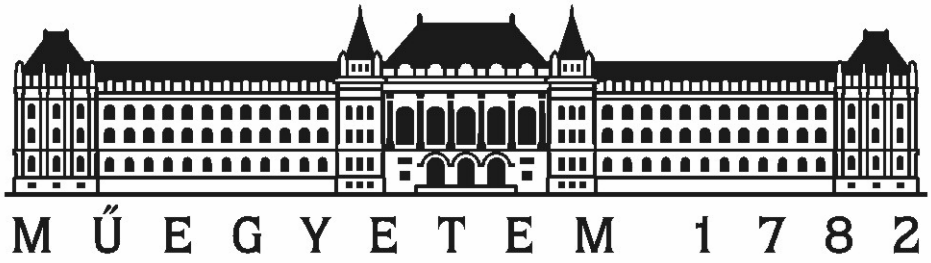

Budapesti Műszaki és Gazdaságtudományi Egyetem
Irányítástechnika és Informatika Tanszék

TARTALOMAZONOSÍTÁSI SZTEGANOGRÁFIAI MÓDSZEREK

című doktori értekezés tézisei

Lenti József

Témavezető:
Dr. Loványi István
egyetemi docens
BMGE Irányítástechnika és Informatika Tanszék

Budapest 2005

1 Bevezetés

Manapság egyre több dokumentumot használunk és kezelünk digitális formátumban. A digitálisan tárolt dokumentumok, audió és videó anyagok esetében a kalózkodásnak – a dokumentumok illegális terjesztésének és másolásának – egyre nagyobb a veszélye. Addig, amíg a digitális formában történő kezelés nem terjedt el, a különböző multimédia anyagokat lehetett ugyan másolni, azonban minden egyes másolás után minőségromlás következett be, azaz az eredeti anyaghoz képest minőségileg rosszabb lett a másolt változat. A digitálisan tárolt dokumentumok esetében azok másolása minőségvesztés nélkül történhet meg, és a másolás elvégzéséhez nem szükséges költséges berendezések beszerzése. A digitális dokumentumok illegális terjesztése is könnyebb, mint az analógoké – számítógépes hálózatokon keresztül ma is igen nagy mennyiségű „kétes eredetű" dokumentumot terjesztenek.

A digitális anyagok nemcsak az eredeti formátumukban, hanem azt átalakítva, tömörítve is továbbíthatók. A különböző formátumokban tárolt anyagok gyakorlatilag az eredeti formátumú anyaggal azonos felhasználhatóságot tudnak biztosítani. A multimédia anyagok esetében az azonosítás és integritás ellenőrzés ma több területen is egyre fontosabb szempont. A tartalomazonosítás több célra is használható, például tárgyalási eljárásokban, egészségügyi alkalmazásokban, elektronikus kereskedelemben – abban az esetben, amikor valamilyen szempontból biztosak szeretnénk lenni abban, hogy a látott digitális formátumú kép, videó vagy audió anyag autentikus. Természetesen a különböző célú alkalmazások esetén az elvárások illetve az alkalmazott módszerek eltérhetnek. Az azonosítás során tág értelemben általában három főbb paraméter vizsgálata történik meg: az adat integritásának, az adat forrásának valamint az adat valódiságának vizsgálata.

Számos esetben – például orvosi képek esetében – szükséges, hogy meg lehessen győződni egy adott digitális anyag sértetlenségéről, azaz arról, hogy az valóban eredeti-e, illetve nem módosítottak-e azon a felvételt illetve a kibocsátást követően. Ennek egy lehetséges módja az lehet, ha csatolt információként különböző kriptográfiai módszerekkel biztosítják a kívánt feltételek ellenőrizhetőségét. Egy másik, ennél sokkal megbízhatóbb megoldás az, amikor magába az anyagba ágyazzák be azt az információt, mely szükséges ahhoz, hogy annak eredetiségét vizsgálni lehessen.

A multimédia anyagok azonosítása, azok integritásellenőrzése eltér a hagyományos „üzenetek” ellenőrzésétől. A multimédia anyagok a legtöbb esetben különböző szabványok szerinti formátumban – mint például JPEG, MPEG, FLAC – kerülnek továbbításra. A legtöbb alkalmazás esetében a tömörített és az eredeti formátumú anyag azonosnak tekinthető – mint például az eredeti DVD-n forgalmazott film, valamint az annak AVI formátumban illegálisan terjesztett változata.

A multimédia anyagok azonosítása általános értelemben megtehető kriptográfiai és szteganográfiai módszerekkel. A kriptográfiai módszerek közül általában a különböző üzenet azonosítási technikákat alkalmazzák az azonosításhoz. A tartalom azonosítás esetében nem pusztán üzenet azonosításról van szó. Üzenet azonosítás esetében a vizsgált szempont az, hogy az eredeti üzenet sértetlensége fennáll-e, azaz a vizsgált és az eredeti üzenet bitről bitre megegyezik-e. Az üzenetazonosítás vizsgálatára több kriptográfiai megoldás létezik, a leggyakrabban alkalmazott megoldás a digitális aláíráson alapul. A digitális aláírás az eredeti anyaghoz csatolt, de fizikailag külön kezelt adathalmaz.

A vízjelezés esetében a multimédia anyagot magát tekintik kommunikációs csatornának. Ebbe a csatornába ágyazott vízjel információ tartalmazhatja az anyag tulajdonosának adatait vagy annak azonosításához szükséges tartalomfüggő információt. A multimédia azonosítás esetében nem az anyag bitről-bitre való azonosítása a cél, hanem az abban foglalt tartalom azonosítása, ahol az eredeti tartalom valamilyen módon módosulhatott, például annak módosításával vagy veszteséges tömörítés alkalmazásával. Természetesen a tartalomazonosításnál meg kell határozni azokat a limiteket, melyek megszabják, hogy az eredeti tartalom mely mértékű módosítása tekinthető még elfogadhatónak, mely mértékű módosulás esetén tekinthető az eredetivel azonosnak.

A hagyományos, digitális aláíráson alapuló tartalomazonosítás semmilyen mértékű módosítást nem tesz lehetővé. A hagyományos vízjelezési megoldások fő tervezési szempontja az, hogy a lehető legnagyobb mértékű módosítás esetén is detektálható legyen a beágyazott információ, adott esetben még a tartalom bizonyos részeinek megváltoztatása esetén is. A tartalomazonosítási feladatokra ma a legelfogadottabb megoldások a félig törékeny vízjel-beágyazási eljárások. A vízjelezési megoldások preferáltak a tartalomazonosítás esetén, hiszen az ahhoz használt információ az eredeti multimédia tartalomba ágyazódik, annak szerves részét képezi.

2 Kitűzött kutatási feladatok

A képek azonosításának, sértetlenségének vizsgálatához használt vízjel információk általában az adott kép tartalmi elemeitől függenek, különböző képi tulajdonságok alapján történik azok meghatározása. Ebben az esetben a vízjel információ arra használható fel, hogy vizsgálni lehessen annak alapján a kép sértetlenségét [4]. A nemzetközi irodalomban több megoldást is javasolnak az orvosi képek integritásának biztosítására szteganográfiai eszközökkel [12, 14]. A beágyazott információval kapcsolatban nem csak a biztonságosság a követelmény orvosi alkalmazások esetében, hanem az is, hogy lehetőleg a vízjelezés során az eredeti kép csekély mértékben módosuljon – mely függ a kiválasztott beágyazási módszertől, illetve a beágyazott információ méretétől – valamint az, hogy a beágyazási technika törölhető legyen, azaz a beágyazott vízjelet el lehessen távolítani az ellenőrzés során [2, 3, 10, 11, 13]. Kutatási célkitűzésem az volt, hogy egy olyan beágyazott vízjel információt alakítsak ki, mely kapcsolódik a kép tartalmi elemeihez, valamint a képhez csatolt egyéb információkhoz és segítségével lehetséges legyen a kép integritásellenőrzése.

A vízjel információ kialakítása során fontos az a tulajdonság, hogy a vízjel a kép mely mértékű módosítása után nyerhető ki az adott képből. Egy adott képen többféle módosítást lehet elvégezni, melyek a képi tartalmat befolyásolhatják. A tulajdonjog védelem esetén természetesen a kép jogos tulajdonosának a vízjel információ beágyazásával a célja az, hogy, a beágyazott információt ne lehessen eltávolítani az adott képből lehetőleg annak sorozatos módosítását követően sem. Ebben az esetben általában a beágyazott információ nem kötődik a képi tartalomhoz, azaz maga a beágyazott információ illetve a kép által hordozott képi információ között nincs összefüggés [5, 7]. Tartalom azonosítás esetében azonban szükséges annak meghatározása, hogy a tartalom milyen típusú módosítása esetén tekinthetjük azt az eredetivel azonosnak. Természetesen, ha nem tennénk meg ezt a megkülönböztetést, akkor a tartalom azonosítás problémaköre azonos lenne az üzenet azonosítással [9, 18]. Amennyiben képek esetében csak az eredetivel teljesen megegyező képeket tekintenénk tartalom azonosítás szempontjából azonosnak, úgy a kép bármely pixelének módosítása esetén is a tartalomazonosítási folyamat két különböző képet jelezne. Természetesen bizonyos esetekben ilyen pontosságú megkülönböztetés is

fontos lehet, azonban a legtöbb alkalmazás esetében a tartalomazonosítás olyan megoldása szükséges, ahol megengedhető az eredeti média bizonyos határok közti módosítása [16]. Ma a szteganográfiai megoldások között a tartalomazonosítás a leginkább kutatott terület [1, 15, 17].
Célom egy olyan algoritmus kifejlesztése volt, ahol a tartalomazonosítás során a JPEG transzformáció az elfogadható módosítás. A kutatási célkitűzésem egy olyan algoritmus kialakítása volt, melynek felhasználásával az eredeti kép JPEG tömörített változata is azonosítható, illetve a módszer segítségével detektálhatóak azok a képblokkok, melyek az eredeti képhez képest módosításra kerültek.

A vízjel információ beágyazási módszerei az alkalmazott terület követelményeinek megfelelően különbözőek lehetnek. A beágyazási módszerek között megkülönböztetünk robosztus, törékeny illetve félig törékeny beágyazási módszereket. A félig törékeny algoritmusok esetében a cél az, hogy a beágyazás során elrejtett információ meghatározott képmódosításoknak ellenálljon, azonban a más módosításokkal szembeni ellenálló képesség ez esetben marginális szempont. Általánosságban elmondható, hogy az ilyen típusú vízjelek adott típusú manipulációkkal szemben ellenállóak, a legtöbb szándékos módosítási kísérlet esetén a beágyazott vízjel sérül. Ebben az esetben a cél nem a tulajdonos jogainak a védelme, hanem elsősorban az azonosítási célok, így ebben az esetben a kép azonosítása történik meg oly módon, hogy az eredeti képhez képest adott típusú módosításokat lehet megengedhetőnek tekinteni.
Célom egy olyan vízjel beágyazó algoritmus kerül kialakítása volt, mely a félig törékeny beágyazási kategóriába tartozik. Az algoritmus az adott minőségi faktorral végrehajtott JPEG tömörítés esetén garantálja a beágyazott vízjel sértetlenségét, illetve felhasználásával törölhető vízjel információt lehet a képekbe ágyazni.

3 Új tudományos eredmények

1. tézis: Kifejlesztettem egy fix hosszúságú, integritás- és tulajdonosazonosításhoz felhasználható vízjel információt generáló algoritmust [L6]

Az algoritmus lényeges újítása az, hogy a beágyazott vízjel információ nem csak a képi, hanem a képhez csatlakozó egyéb adatokhoz is kapcsolódik. A korábbi megközelítések esetében a beágyazott, integritás ellenőrzéshez használható vízjel alapján a tulajdonosi jogok nem igazolhatók [1, 2, 10], a kifejlesztett algoritmus felhasználásával a tulajdonosi jogok igazolása megtehető. A kifejlesztett algoritmus által generált vízjel információ felhasználható robosztus, törékeny illetve félig törékeny típusú vízjel információ vízjel beillesztésénél. A kialakított algoritmus kép-specifikus tulajdonságok alapján előállít egy olyan azonosítót, mely a következő főbb tulajdonságokkal rendelkezik:

- A kép egyedi azonosítójaként használható, azaz használható képi adatbázisban a képhez tartozó azonosítóként. Mivel az információ vízjel információként a képbe is beágyazásra kerül, így lehetséges egy vízjelezett kép alapján a képhez tartozó adatbázis-rekordok meghatározása. Orvosi adatbázisokban, ahol a képek – például méretük miatt – nem az adatbázisban, hanem különálló file-okban vannak eltárolva ez a nemzetközi orvosinformatikai ajánlások alapján kiemelt feladat.
- Alkalmas a kép integritásának ellenőrzésére, azaz felhasználásával lehetséges annak megállapítása, hogy a kép módosításra került-e
- Kapcsolatot teremt a kép, illetve a képhez kapcsolódó egyéb adatok között
- Az algoritmusnak köszönhetően a képzett vízjel információ egy rövid, fix hosszúságú bitsorozat, a képzett képi azonosító a kép méretétől független, az algoritmusban használt paraméterek beállításának függvénye. Vízjelezés esetében kiemelten fontos, hogy a beágyazott információ mérete lehetőség szerint minimális legyen a beágyazási folyamat által okozott módosítás minimalizálása érdekében.
- A tulajdonosi jogok igazolhatóak felhasználásával, azaz a kép tulajdonosa a beágyazott vízjel információval igazolni tudja, hogy az adott kép valóban az ő tulajdona.
- Az algoritmus felhasználásával kialakított vízjel információ felhasználása esetén a vízjelezett kép ellenáll a vízjelmásoláson alapuló támadásoknak.

2. tézis: Kifejlesztettem egy új, képek tartalom azonosításához felhasználható vízjel információként felhasználható tulajdonság-vektort generáló algoritmust. [L9]

Kifejlesztettem egy olyan szteganográfiai tartalomazonosításhoz használható algoritmust, melynek segítségével előállítható olyan tulajdonság-vektor, mely alapján lehetséges képek tartalom azonosítása a tömörített kép esetében is. Ugyan léteznek olyan megoldások melyek felhasználásával a tartalomazonosítás tömörített képek esetén is lehetséges [13, 15, 18], a kifejlesztett algoritmus azonban képes arra, hogy meghatározza azokat a képblokkokat amelyek módosításra kerültek az eredeti képhez képest. Ez azt jelenti, hogy a kifejlesztett algoritmus lehetővé teszi, hogy megkülönböztesse a kép szándékos módosítását – mely lehet a kép tartalmának módosítása – a kép veszteséges tömörítésétől, így a tartalom azonosítás megtehető az adott kép veszteségesen tömörített változata esetében is. Az algoritmus a tulajdonság-vektor generálását végző és a tulajdonság-vektor alapján a tartalomazonosítást végző folyamatból áll.
A tartalomazonosítás során az elfogadható módosítás, melyet követően a kép a tulajdonság-vektor alapján azonosítható, a JPEG tömörítés. Azaz az eredeti, tömörítetlen képből képzett tulajdonság-vektor alapján lehetséges az eredeti kép illetve annak JPEG tömörített változatának tartalom azonosítása is.
A kifejlesztett algoritmus által biztosított legjelentősebb újítás az, hogy a tartalomazonosítás során az egyes képrészletek tartalomazonosítása történik meg, azaz a generált tulajdonság-vektor alapján nem csak a tartalomazonosítás végezhető el, hanem lehetséges a kép azon régióinak meghatározása, melyek az eredeti képhez képest módosultak. Az ellenőrzés során kijelölhetőek azon képblokkok, melyek az eredeti képhez képest módosultak, tehát meghatározhatóak azon régiók, ahol a kép tartalma az eredetihez képest megváltozott.

3. tézis: Kifejlesztettem egy törölhető, félig törékeny vízjel beágyazó algoritmust, mely félig törékeny az adott minőségi faktorú JPEG tömörítéssel szemben [L7, L8]

Kifejlesztettem egy olyan szteganográfiai, törölhető, félig törékeny beágyazó algoritmust, melynek segítségével lehetséges biztonságos módon információ

beágyazása digitális képekbe. Amennyiben a kép tartalomazonosításához szükséges információ vízjelként kerül beágyazásra és a tartalomazonosítás során a megengedett módosítás a veszteséges JPEG tömörítés, akkor célszerű olyan beágyazó algoritmus használata, mely félig törékeny a tartalomazonosítás során megengedett módosítástípussal szemben.

Az algoritmus félig törékeny a JPEG tömörítéssel szemben, azaz az adott minőségi faktorral végrehajtott JPEG tömörítés esetén garantálja a beágyazott vízjel sértetlenségét, illetve felhasználásával törölhető vízjel információt lehet a képekbe ágyazni.

A bemutatott algoritmus felhasználható olyan tartalom azonosításhoz használt vízjel információ beágyazására, melynek során követelmény a JPEG tömörítéssel szembeni félig törékeny tulajdonság. A kifejlesztett algoritmus leglényegesebb újítása az, hogy a JPEG tömörítésnél használt minőségi faktor, mellyel szemben a félig törékeny tulajdonság fennáll az algoritmus paramétereként beállítható, ezáltal a vízjel beillesztés által okozott képmódosítás minimalizálható a tömörítéssel szemben elvárt ellenállóképesség függvényében. A paraméterként beállított minőségi faktornál nagyobb minőségi faktorú JPEG tömörítés esetében beágyazott vízjel kiolvasása sikeres, azaz a JPEG tömörítés során a beágyazott információ nem sérülhet.

A beágyazási algoritmus törölhető, azaz a vízjel kiolvasást követően a beágyazott információ eltávolítható, az eredeti, módosítatlan kép pedig a kiolvasást követően helyreállítható. A kifejlesztett algoritmus az általánosan használt törölhető vízjel megoldásoknál [1, 6, 9] kisebb mértékben módosítja a vízjelezendő képet, hiszen a beállított minőségi faktorérték miatt csak a minimálisan szükséges módosításokat hajtja végre az információ beágyazás során.

4 Eredmények alkalmazása

Az Irányítástechnika és Informatika Tanszék, a BULL Magyarország Kft. illetve a Vasútegészségügyi Kht. közös munkája az „IKTA3 144/2000 Integrált egészségügyi informatikai rendszerek” elnevezésű projekt. A projekt során portábilis, képeket is tartalmazó orvosi betegrekordok a kialakítása volt a cél, melyek alapjául szolgálhatnak több orvosinformatikai rendszer közti kommunikáció kialakításának. A

projekt során kiemelt fontosságú volt a biztonsági kérdések kezelése, a továbbított orvosi képek, felvételek integritásának vizsgálata. Az első tézis ezen munka keretein belül került kialakításra, illetve felhasználásra a projektben.

A „Balaton" magyar- francia kormányközi kutatási program keretében bilaterális együttműködés alakult ki a Budapesti Műszaki és Gazdaságtudományi Egyetem és az ENST Bretagne között. Az együttműködés keretein belül a főbb fókuszpontok a telediagnosztika, orvosi képfeldolgozás és képkompresszió. Tekintettel arra, hogy a kialakított rendszerek között szerepelnek oktatási célokat szolgáló orvosi rendszerek, így az orvosi képek tulajdonosazonosításán túl azok tartalomazonosítása is szükséges volt a az orvosi képek jogosult felhasználásának ellenőrzése érdekében. A második és a harmadik tézis e munkához kapcsolódva született meg, ezen túlmenően az IKTA4 138/2001 „Humán mozgások analízise 3D módszerekkel" projekt keretein belül is felhasználásra kerül.

5 Hivatkozások

[1] N. F. Johnson, Z. Duric, and S. Jajodia. Information Hiding: Steganograph and Watermarking - Attacks and Countermeasures. Kluwer Academic Press, Dordrecht, the Netherlands, 2001.

[2] X. Kong and R. Feng. Watermarking medical signals for telemedicine. IEEE Trans on. information Technology in Biomedicine, 5(3):195–201, Sept. 2001.

[3] H. Tachibana, H. Harauchi, T. Ikeda, Y. Iwata, A. Takemura, and T. Umeda. Practical use of new watermarking and vpn techniques for medical image communication and archive. RSNA 2002 Archive Site: http://archive.rsna.org/index.cfm

[4] A.Wakatani. Digital watermarking for ROI medical images by using compressed signature image. In Annual Hawaii Int. Conf. on System Sciences, pages 2043– 2048, Hawaii, USA, Jan. 2002.

[5] Ingemar Cox, Matthew Miller, Jeffrey Bloom, Digital watermarking. Morgan Kaufmann Publishers, 2001

[6] J. Friedrich, M. Goljan and M. Du, "Invertible Authentication", "Proceedings of SPIE, Security and Watermarking of Multimedia Contents", 2001

[7] Jozsef Lenti, Istvan Lovanyi. "Image integrity verification in medical information systems", "Proceeding of MIE2003, The New Navigators: from Professionals to Patients, Medical Image Information Systems", pp 286-291

[8] Bruce Schneier. Applied cryptography Second Edition. John Whiley and Sons Inc. 1996

[9] M. M. Yeung and F.Mintzer, An invisible watermarking technique for image verification, in Proc. IEEE International Conference on Image Processing, vol. 2, pp. 680–683, Santa Barbara, California, USA, October 1997.

[10]G. Coatrieux, B. Sankur, H. Maitre, Strict Integrity Control of Biomedical Images, SPIE Conf. 4314: Security and Watermarking of Multimedia Contents III, 22-25 Jan. 2001, San Jose USA

[11]N.J.G. Brown, K.E. Britton, D.L. Plummer: Standardisation in medical image management International Journal of Medical Informatics 48, 1998, pp 227-238

[12]G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec. Relevance of Watermarking in Medical Imaging. 2000 IEEE EMBS Conf. On Information Technology Applications in Biomedicine, Nov. 2000, Arlington, USA. , p 250-255

[13]F. Mintzer, G.W. Braudaway, and M. M. Yeung. Effective and ineffective digital watermarks. IEEE ICIP, volume III, Santa-Barbara, Cal, October 1997, pages 9—12

[14]Lesley R. Matheson, Stephen G. Mitchell, Talal G. Shamoon, Robert E. Tarjan, Francis Zane, Robustness and security of digital watermarks, Financial Cryptography FC-98, volume 1465 of Lecture Notes in Computes Science, Springer, 1998, pages 227-240

[15]S. Bhattacharjee and M. Kutter, Compression Tolerant Image Authentication, IEEE International Conf. on Image Processing, Chicago, October 1998.

[16]M. L. Miller, I. J. Cox and J. A. Bloom, Informed Embedding Exploiting Image and Detector Information during Watermark Insertion, IEEE Intl. Conf. on Image Processing, Vol. 3, pp.1-4, September 2000.

[17]T. Uehara and R. Safavi-Naini, On (In) security of 'A Robust Image Authentication Method', Proc. IEEE Pacific Rim Conf. on Multimedia, pp. 1025-1032, Dec. 2002.

[18]M. Wu and B. Liu, "Watermarking for Image Authentication," IEEE Proc. of ICIP, Chicago, Oct 1998.

6 Publikációk

[L1] Lenti József, Steganographic Methods, Periodika Polytechnika, Electrical Engineering, Hungary, 2000 44/3-4, 249-258 oldal

[L2] Dr. Loványi István, Lenti József, Y2K – ezredfordulón túlmutató kihatások, Egészségügyi Menedzsment, 1999 október 1, 52-54 old.

[L3] Lenti József, Biztonság és hatékonyság, Computerworld - Számítástechnika, XVII évfolyam 39. szám, 2002 szeptember 24, 22. old

[L4] Lenti József, Staganographic methods, MicroCAD2000, Miskolc International Science Conference, 54-61 oldal, 2000 február 23-24

[L5] Lenti József, Loványi István, Nagy Ákos, Blind Signature Based Steganographic Protocol, I. Magyar Számítógépes Grafika és Geometria Konferencia, Budapest 2002 május 28-29, 133-139 oldal

[L6] Jozsef Lenti, István Loványi, Image Integrity Verification in Medical Information Systems, MIE2003, Proceedings of Medical Informatics Europe 2003, 4-7 May , 2003 Saint-Malo, France, pp. 286-291

[L7] Lenti József, Loványi István, Dezső Zoltán, Efficient Watermark Embedding in Medical Images, IEEE Conference – 2004 International Conference on Intelligent Engineering Systems, 2004 september 19-21, Cluj-Napoca, Romania, pp. 232-235

[L8] József Lenti, István Loványi, Erasable, Semi-fragile Watermark Embedding Process for Images, IEEE 9th International Conference on Intelligent Engineering Systems, 16-19 September, 2005

[L9] József Lenti, István Loványi, Feature Vector Generation for Image Integrity Verification, IEEE 9th International Conference on Intelligent Engineering Systems, 16-19 September, 2005

[L10] Z. Dezső, G. Bálint, A. Hunka, J. Lenti, I. Lovanyi Motion Capture vs. traditional medical examinations SETIT 2005 27-31 Mars 2005 Sousse – Tunisie, Actes de SETIT 2005 p. 106.